Cisco Router and Security Device Manager User's Guide

2.5

C O N T E N T S

Cisco Router and Security Device Manager 2.5 User's Guide

Home Page

The home page supplies basic information about the router hardware, software, and configuration. This page contains the following sections:

Host Name

The configured name of the router.

About Your Router

Shows basic information about your router hardware and software, and contains the following fields:

Hardware		Software	
Model Type	Shows the router model number.	**IOS Version**	The version of Cisco IOS software that is currently running on the router.
Available/Total Memory	Available RAM/Total RAM	**Cisco SDM Version**	The version of Cisco Router and Security Device Manager (Cisco SDM) software that is currently running on the router.

Hardware		Software	
Total Flash Capacity	Flash plus Webflash (if applicable)		
Feature Availability	The features available in the Cisco IOS image the router is using are designated by a check. The features Cisco SDM checks for are: IP, Firewall, VPN, IPS, and NAC.		

More...

The **More...** link displays a popup window providing additional hardware and software details.

- Hardware Details—In addition to the information presented in the About Your Router section, this tab displays information about:

  – Where the router boots from–Flash or Configuration File.

  – Whether the router has accelerators, such as VPN accelerators.

  – A diagram of the hardware configuration, including flash memory and installed devices such as USB flash and USB tokens.

- Software Details—In addition to the information presented in the About Your Router section, this tab displays information about:

  – The feature sets included in the IOS image.

  – The version of Cisco SDM running.

Configuration Overview

This section of the home page summarizes the configuration settings that have been made.

Note If you do not see feature information described in this help topic on the home page, the Cisco IOS image does not support the feature. For example, if the router is running a Cisco IOS image that does not support security features, the Firewall Policy, VPN, and Intrusion Prevention sections do not appear on the home page.

View Running Config

Click this button to display the router's running configuration.

Interfaces and Connections	Up (*n*): The number of LAN and WAN connections that are up.	Down (*n*): The number of LAN and WAN connections that are down.	Double-arrow head: Click to display/hide details.
Total Supported LAN	The total number of LAN interfaces that are present in the router.	Total Supported WAN	The number of Cisco SDM-supported WAN interfaces that are present on the router.
Configured LAN Interface	The number of supported LAN interfaces currently configured on the router.	Total WAN Connections	The total number of Cisco SDM-supported WAN connections that are present on the router.
DHCP Server	Configured/ Not Configured		
DHCP Pool (Detail view)	If one pool is configured, starting and ending address of DHCP pool. If multiple pools are configured, list of configured pool names.	Number of DHCP Clients (Detail view)	Current number of clients leasing addresses.
Interface	Type	IP/Mask	Description
Name of configured interface	Interface type	IP address and subnet mask	Description of interface

Firewall Policies	Active/Inactive	Trusted (*n*)	Untrusted (*n*)	DMZ (*n*)
	Active—A firewall is in place. Inactive—No firewall is in place.	The number of trusted (inside) interfaces.	The number of untrusted (outside) interfaces.	The number of DMZ interfaces.

Cisco Router and Security Device Manager 2.5 User's Guide

Firewall Policies	Active/Inactive	Trusted (*n*)	Untrusted (*n*)	DMZ (*n*)
Interface	Firewall Icon	NAT	Inspection Rule	Access Rule
The name of the interface to which a firewall has been applied	Whether the interface is designated as an inside or an outside interface.	The name or number of the NAT rule applied to this interface.	The names or numbers of the inbound and outbound inspection rules.	The names or numbers of the inbound and outbound access rules.

VPN	**Up** (*n*)- The number of active VPN connections.		
IPSec (Site-to-Site)	The number of configured site-to-site VPN connections.	**GRE over IPSec**	The number of configured GRE over IPSec connections.
Xauth Login Required	The number of Easy VPN connections awaiting an Xauth Login. *See note*.	**Easy VPN Remote**	The number of configured Easy VPN Remote connections.
No. of DMVPN Clients	If router is configured as a DMVPN hub, the number of DMVPN clients.	**No. of Active VPN clients**	If this router is functioning as an Easy VPN Server, the number of Easy VPN clients with active connections.
Interface	**Type**	**IPSec Policy**	**Description**
The name of an interface with a configured VPN connection	The type of VPN connection configured on the interface.	The name of the IPSec policy associated with the VPN connection.	A description of the connection.

✎

Note
- Some VPN servers or concentrators authenticate clients using Extended Authentication (XAuth). This shows the number of VPN tunnels awaiting an Xauth login. If any Easy VPN tunnel awaits XAuth login, a separate message panel is shown with a Login button. Clicking **Login** allows you to enter the credentials for the tunnel.

- If Xauth has been configured for a tunnel, it will not begin to function until the login and password has been supplied. There is no timeout after which it will stop waiting; it will wait indefinitely for this information.

NAC Policies	Active or Inactive
Interface Column	**NAC Policy Column**
The name of the interface to which the policy is applied. For example, FastEthernet 0, or Ethernet 0/0.	The name of the NAC policy.

Routing		Intrusion Prevention	
No. of Static Routes	The number of static routes configured on the router.	**Active Signatures**	The number of active signatures the router is using. These may be built in, or they may be loaded from a remote location.
Dynamic Routing Protocols	Lists any dynamic routing protocols that are configured on the router.	**No. of IPS-enabled interfaces**	The number of router interfaces on which IPS has been enabled.

Routing		Intrusion Prevention	
		SDF Version	The version of SDF files on this router.
		Security Dashboard	A link to the IPS Security Dashboard, where the top-ten signatures can be viewed and deployed.

Creating a New Connection

The Cisco SDM connection wizards guide you LAN and WAN configurations, and check the information that you enter against the existing configuration, warning you of any problems.

This chapter contains the following sections:

- Creating a New Connection
- New Connection Reference
- Additional Procedures

Creating a New Connection

Complete these steps to create a new connection:

Step 1 On the Cisco SDM toolbar, click **Configure**.

Step 2 On the Tasks bar, click Interfaces and Connections.

Step 3 In the Create New Connection box, choose the type of connection that you want to configure. Information about the type of connection you choose is displayed in the Information box, and the Use Case Scenario area displays a graphic showing the kind of connection that you chose.

Step 4 Click **Create New Connection** to get started.

New Connection Reference

The following topic describes the screen referred to in this chapter:

- Create Connection

Create Connection

This window allows you to create new LAN and WAN connections.

✎ **Note**   You cannot use Cisco SDM to create WAN connections for Cisco 7000 series routers.

Field Reference

Table 2-1 describes the fields in this screen.

Table 2-1   *Create Connection Fields*

Element	Description
Create New Connection	Choose a connection type to configure on the physical interfaces available on your router. Only interfaces that have not been configured are available. If all interfaces have been configured, this area of the window is not displayed.
	If the router has Asynchronous Transfer Mode (ATM) or serial interfaces, multiple connections can be configured from a single interface because Cisco Router and Security Device Manager II (Cisco SDM) configures subinterfaces for each interface of that type.
	The Other (Unsupported by Cisco SDM) radio button appears if an unsupported logical or physical interface exists, or if a supported interface exists that has been given an unsupported configuration. When you click the Other (Unsupported by Cisco SDM) radio button, the Create New Connection button is disabled.

Table 2-1   Create Connection Fields

Element	Description
	If the router has radio interfaces but you do not see a **Wireless** radio button, you are not logged on as an Cisco SDM Administrator. If you need to use the wireless application, go to the Cisco SDM Tools menu and choose **Wireless Application**.
Use Case Scenario	When you click the radio button for a connection type, a network diagram appears illustrating that type of connection.
Information	The information area displays more information about the connection type you choose. For example, if you choose Ethernet LAN, theinformation area may display the text "Configure Ethernet LAN interface for straight routing and 802.1q trunking."
Create New Connection button	Click **Create New Connection** to start the wizard for the type of connection you chose.

Additional Procedures

This section contains procedures for tasks that the wizard does not help you complete.

This section contains the following topics:

- How Do I Configure a Static Route?
- How Do I View Activity on My LAN Interface?
- How Do I Enable or Disable an Interface?
- How Do I View the IOS Commands I Am Sending to the Router?
- How Do I Configure an Unsupported WAN Interface?
- How Do I Enable or Disable an Interface?
- How Do I View Activity on My WAN Interface?
- How Do I Configure NAT on a WAN Interface?
- How Do I Configure a Static Route?
- How Do I Configure a Dynamic Routing Protocol?

- How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

How Do I Configure a Static Route?

To configure a static route:

Step 1   From the task bar, click **Routing**.

Step 2   In the Static Routing group, click **Add...**.

The Add IP Static Route dialog box appears.

Step 3   In the Prefix field, enter the IP address of the static route destination network.

Step 4   In the Prefix Mask field, enter the subnet mask of the destination network.

Step 5   If you want this static route to be the default route, check the **Make this as the Default Route** check box.

Step 6   In the Forwarding group, select whether to identify a router interface or the destination router IP address as the method to forward data, and then choose either the forwarding router interface or enter the destination router IP address.

Step 7   Optionally, in the Distance Metric field, enter the distance metric to be stored in the routing table.

Step 8   If you want to configure this static route to be a permanent route, which means that it will not be deleted even if the interface is shut down or the router is unable to communicate with the next router, check the **Permanent Route** check box.

Step 9   Click **OK**.

How Do I View Activity on My LAN Interface?

You can view activity on a LAN interface by using the Monitor mode in Cisco SDM. Monitor mode can display statistics about the LAN interface, including the number of packets and bytes that have been sent or received by the interface, and the number of send or receive errors that have occurred. To display statistics about about a LAN interface:

Step 1   From the toolbar, click **Monitor**.

Step 2   From the left frame, click **Interface Status**.

Step 3   In the Select an Interface field, select the LAN interface for which you want to view statistics.

Step 4   Select the data item(s) you want to view by checking the associated check box(es). You can view up to four statistics at a time.

Step 5   Click **Start Monitoring** to see statistics for all selected data items.

The Interface Details screen appears, displaying the statistics you selected. The screen defaults to showing real-time data, for which it polls the router every 10 seconds. If the interface is up and there is data transmitting across it, you should see an increase in the number of packets and bytes transferred across the interface.

How Do I Enable or Disable an Interface?

You can disable an interface without removing its configuration, and you can reenable an interface that you have disabled.

Step 1   Click **Interfaces and Connections** in the task bar.

Step 2   Click the **Edit Interfaces and Connections** tab.

Step 3   Select the interface that you want to disable or enable.

Step 4   If the interface is enabled, the Disable button appears below the Interface List. Click that button to disable the interface. If the interface is currently disabled, the Enable button appears below the Interface List. Click that button to disable the interface.

How Do I View the IOS Commands I Am Sending to the Router?

If you are completing a Wizard to configure a feature, you can view the Cisco IOS commands that you are sending to the router when you click **Finish**.

Step 1   From the Cisco SDM Edit menu, select **Preferences**.

Step 2   Check **Preview commands before delivering to router.**

Step 3   Click **OK**.

The next time you use a wizard to configure the router and click **Finish** on the Summary window, the Deliver window will appear. In this window you can view the commands that you are delivering to the router's configuration. Click **Deliver** when you are finished reviewing the commands.

If you are editing a configuration, the Deliver window is displayed when you click **OK** in the dialog window. In this window you can view the Cisco IOS commands that you are sending to the router .

How Do I Launch the Wireless Application from Cisco SDM?

Use the following procedure to launch the wireless application from Cisco SDM.

Step 1   Go to the Cisco SDM Tools menu and select **Wireless Application. The Wireless Application launches in a separate browser window.**

Step 2   In the left panel, click the title of the configuration screen that you want to work in. To obtain help for any screen, click the help icon in the upper right corner. This icon looks like an open book with a question mark.

How Do I Configure an Unsupported WAN Interface?

Cisco SDM does not support configuration of every WAN interface that your router might support. If Cisco SDM discovers an interface in your router that it does not support, or a supported interface with an unsupported configuration, Cisco SDM displays a radio button labeled Other (Unsupported by Cisco SDM). The unsupported interface is displayed in the Interfaces and Connections window, but it cannot be configured using Cisco SDM.

To configure an unsupported interface, you must use the router command-line interface (CLI).

How Do I Enable or Disable an Interface?

You can disable an interface without removing its configuration, and you can reenable an interface that you have disabled.

Step 1   Click **Configure** on the Cisco SDM toolbar.

Step 2   Click **Interfaces and Connections** in the left frame.

Step 3   Click the interface that you want to disable or enable.

Step 4   If the interface is enabled, the Disable button appears below the Interface List. Click it to disable the interface. If the interface is currently disabled, the Enable button appears in that location. Click that button to disable the interface.

How Do I View Activity on My WAN Interface?

You can view activity on a WAN interface by using the Monitor feature in Cisco SDM. Monitor screens can display statistics about the WAN interface, including the number of packets and bytes that have been sent or received by the interface, and the number of send or receive errors that have occurred. To display statistics about a WAN interface:

Step 1   From the toolbar, click **Monitor**.

Step 2   From the left frame, click **Interface Status**.

Step 3   In the Select an Interface field, choose the WAN interface for which you want to view statistics.

Step 4   Choose the data item(s) you want to view by checking the associated check box(es). You can view up to four statistics at a time.

Step 5   Click **Show Details** to see statistics for all selected data items.

The Interface Details screen appears, displaying the statistics you selected. The screen defaults to showing real-time data, for which it polls the router every 10 seconds. If the interface is up and there is data transmitting across it, you should see an increase in the number of packets and bytes transferred across the interface.

How Do I Configure NAT on a WAN Interface?

Step 1   Click **Configure** on the Cisco SDM toolbar.

Step 2   Click **NAT** in the left frame.

Step 3   In the NAT window, click **Designate NAT interfaces**.

Step 4   Find the interface for which you want to configure NAT.

Step 5   Check **inside(trusted)** next to the interface to designate the interface as an inside, or trusted interface. An inside designation is typically used to designate an interface serving a LAN whose resources. must be protected. Check **outside(untrusted)** to designate it as an outside interface. Outside interfaces typically connect to an untrusted network. Click **OK**.

The interface is added to the pool of interfaces using NAT.

Step 6   Review the Network Address Translation Rules in the NAT window. If you need to add, delete, or modify a rule, click the appropriate button on the NAT window to perform the configuration you need.

For more information, click the following links:

- Add or Edit Static Address Translation Rule: Inside to Outside
- Add or Edit Static Address Translation Rule: Outside to Inside
- Add or Edit Dynamic Address Translation Rule: Inside to Outside
- Add or Edit Dynamic Address Translation Rule: Outside to Inside

How Do I Configure NAT on an Unsupported Interface?

Cisco SDM can configure Network Address Translation (NAT) on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is "Up."

After you have configured the unsupported interface using the CLI, you can configure NAT using Cisco SDM. The unsupported interface will appear as "Other" on the router interface list.

How Do I Configure a Dynamic Routing Protocol?

To configure a dynamic routing protocol:

Step 1   From the toolbar, click **Configure**.

Step 2   From the left frame, click **Routing**.

Step 3   In the Dynamic Routing group, click the dynamic routing protocol that you want to configure.

Step 4   Click **Edit**.

The Dynamic Routing dialog box appears, displaying the tab for the dynamic routing protocol you selected.

Step 5   Using the fields in the Dynamic Routing dialog box, configure the dynamic routing protocol. If you need an explanation for any of the fields in the dialog box, click **Help**.

Step 6   When you have finished configuring the dynamic routing protocol, click **OK**.

How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

ISDN BRI and asynchronous connections are dial-up connections, meaning that in order to establish a connection, the router must dial a preconfigured phone number. Because the cost of these types of connections is usually determined by the amount of time that a connection was established, and in the case of an asynchronous connection, that a phone line will be tied up, it is often desirable to configure Dial-on-Demand Routing (DDR) for these connection types.

Cisco SDM can help you configure DDR by:

- Letting you associate a rule (or ACL) with the connection, which causes the router to establish the connection only when it recognizes network traffic that you have identified as interesting with the associated rule.

- Setting idle timeouts, which cause the router to end a connection after a specified amount of time when there is no activity on the connection.

- Enabling multilink PPP, which causes an ISDN BRI connection to use only one of the two B channels unless a specified percentage of bandwidth is exceeded on the first B channel. This has the advantage of saving costs when network traffic is low and the second B channel is not needed, but letting you utilize the full bandwidth of your ISDN BRI connection when needed.

To configure DDR on an existing ISDN BRI or asynchronous connection:

Step 1   Click **Configure** on the Cisco SDM toolbar.

Step 2   Click **Interfaces and Connections** in the left frame.

Step 3   Click the ISDN or asynchronous interface on which you want to configure DDR.

Step 4   Click **Edit**.

The Connection tab appears.

Step 5   Click **Options**.

The Edit Dialer Option dialog box appears.

Step 6   If you want the router to establish the connection only when it recognizes specific IP traffic, click the **Filter traffic based on selected ACL** radio button, and either enter a rule (ACL) number that will identify which IP traffic should cause the router to dial out, or click the **...** button to browse the list of rules and choose the rule that you want to use to identify IP traffic from that list.

Step 7   If you want to configure the router to end the connection when the connection is idle, i.e., no traffic passes across it, for a specified amount of time, in the **Idle timeout** field, enter the number of seconds the connection can remain idle before the router ends the connection.

Step 8   If you are editing an ISDN connection, and you would like to use your second B channel only when the traffic on the first B channel exceeds a certain threshold, check the **Enable MultiLink PPP** check box, then in the **Load Threshold** field, enter a number between 1 and 255, where 255 equals 100% of bandwidth, that will determine the threshold on the first B channel. When traffic on that channel exceeds that threshold, it will cause the router to connect the second B channel. In addition, in the **Data direction** field, you can choose whether this threshold should apply to outbound or inbound traffic.

Step 9   Click **OK**.

How Do I Edit a Radio Interface Configuration?

You must use the Wireless Application to edit an existing radio interface configuration.

Step 1   Click **Configure** on the Cisco SDM toolbar.

Step 2   Click **Interfaces and Connections** in the left frame, and then click the Edit Interface/Connection tab.

Step 3   Choose the radio interface and click **Edit**. In the Connections tab, you can change the IP address or bridging information. If you want to change other wireless parameters, click **Launch Wireless** Application.

Additional Procedures

LAN Wizard

The Cisco Router and Security Device Manager (Cisco SDM) LAN wizard guides you in the configuration of a LAN interface. The screen lists the LAN interfaces on the router. You can select any of the interfaces shown in the window, and click **Configure** to make the interface a LAN interface and configure it.

This window lists the router interfaces that were designated as inside interfaces in Startup configuration, and lists the Ethernet interfaces and switch ports that have not been configured as WAN interfaces. The list includes interfaces that have already been configured.

When you configure an interface as a LAN interface, Cisco SDM inserts the description text $ETH-LAN$ in the configuration file so that it recognizes the interface as a LAN interface in the future.

You can return to this screen as often as necessary to configure additional LAN interfaces.

Field Reference

Table 3-1   IP Address and Subnet Mask

Element	Description
Interface	The name of the interface
Configure	To configure an interface you have selected, click **Configure**. If the interface has not been configured before, Cisco SDM will take you through the LAN Wizard to help you configure it. If the interface has been given a configuration using Cisco SDM, Cisco SDM displays an Edit window enabling you to change configuration settings.
	The Configure button may be disabled if a LAN interface has been given a configuration that Cisco SDM does not support. For a list of such configurations, see Reasons Why an Ethernet Interface Configuration May Be Read-Only.

Ethernet Configuration

The wizard guides you through the configuration of an Ethernet interface on the LAN. You must provide the following information:

- An IP address and subnet mask for the Ethernet interface

- A DHCP address pool if you decide to use DHCP on this interface

- The addresses of DNS and WINS servers on the WAN

- A domain name

LAN Wizard: Select an Interface

Select the interface on which you want to configure a LAN connection in this window. This window lists interfaces that can support Ethernet LAN configurations.

LAN Wizard: IP Address and Subnet Mask

This window lets you configure an IP address and subnet mask for the Ethernet interface that you chose in the first window.

Field Reference

Table 3-2   IP Address and Subnet Mask

Element	Description
IP Address	Enter the IP address for the interface in dotted decimal format. Your network administrator should determine the IP addresses of LAN interfaces. For more information, see IP Addresses and Subnet Masks.
Subnet Mask	Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and host portions of the address. Alternatively, select the number of network bits. This value is used to calculate the subnet mask. Your network administrator can tell you the number of network bits to enter.

LAN Wizard: Enable DHCP Server

This screen lets you enable a DHCP server on your router. A DHCP server automatically assigns reusable IP addresses to the devices on the LAN. When a device becomes active on the network, the DHCP server grants it an IP address. When the device leaves the network, the IP address is returned to the pool for use by another device.

Field Reference

Table 3-3   IP Address and Subnet Mask

Element	Description
Enable DHCP Server	To configure the router as a DHCP server on this interface, click **Yes**.

LAN Wizard: DHCP Address Pool

This screen lets you configure the DHCP IP address pool. The IP addresses that the DHCP server assigns are drawn from a common pool that you configure by specifying the starting IP address in the range, and the ending address in the range.

For more information, see DHCP Address Pools.

Note If there are discontinuous address pools configured on the router, then the Starting IP and Ending IP address fields will be read-only.

Field Reference

Table 3-4   DHCP Address Pool

Element	Description
Starting IP	Enter the beginning of the range of IP addresses for the DHCP server to use in assigning addresses to devices on the LAN. This is the lowest-numbered IP address in the range.
Ending IP	Enter the highest-numbered IP address in the range of IP addresses.
DNS Server and WINS Server Fields	If this window displays DNS Server and WINS Server fields, you can click DHCP Options for information on them.

DHCP Options

Use this window to configure DHCP options that will be sent to hosts on the LAN that are requesting IP addresses from the router. These are not options for the router that you are configuring; these are parameters that will be sent to the requesting hosts on the LAN. To set these properties for the router, click **Additional Tasks** on the Cisco SDM category bar, click **DHCP**, and configure these settings in the DHCP Pools window.

Field Reference

Table 3-5   IP Address and Subnet Mask

Element	Description
DNS Server 1	The DNS server is typically a server that maps a known device name with its IP address. If you have DNS server configured for your network, enter the IP address for that device here.
DNS Server 2	If there is an additional DNS server on the network, you can enter the IP address for that server in this field.
Domain Name	The DHCP server that you are configuring on this router will provide services to other devices within this domain. Enter the name of the domain.
WINS Server 1	Some clients may require Windows Internet Naming Service (WINS) to connect to devices on the Internet. If there is a WINS server on the network, enter the IP address for the server in this field.
WINS Server 2	If there is an additional WINS server on the network, enter the IP address for the server in this field.

LAN Wizard: VLAN Mode

This screen lets you determine the type of VLAN information that will be carried over the switch port. Switch ports can be designated either to be in access mode, in which case they will forward only data that is destined for the VLAN to which they are assigned, or they can be designated to be in trunking mode, in which case they will forward data destined for all VLANs including the VLAN to which they are assigned.

If this switch port will be connected to a single device, such as a single PC or IP phone, or if this device will be connected to a port on a networking device, such as another switch, that is an access mode port, then select **Single Device**.

If this switch port will be connected to a port on a network device, such as another switch, that is a trunking mode, select **Network Device**.

Field Reference

Table 3-6   IP Address and Subnet Mask

Element	Description
Single Device	If this switch port will be connected to a single device, such as a single PC or IP phone, or if this device will be connected to a port on a networking device, such as another switch, that is an access mode port, then choose **Single Device**.
Network Device	If this switch port will be connected to a port on a network device, such as another switch, that is a trunking mode, choose **Network Device**.

LAN Wizard: Switch Port

This screen lets you assign an existing VLAN number to the switch port or to create a new VLAN interface to be assigned to the VLAN switch port.

Field Reference

Table 3-7   IP Address and Subnet Mask

Element	Description
Existing VLAN	If you want to assign the switch port to a VLAN that has already been defined, such as the default VLAN (VLAN 1), enter the VLAN ID number in the Network (VLAN) Identifier field.
New VLAN	If you want to create a new VLAN interface to which the switch port will be assigned, enter the new VLAN ID number in the New VLAN field, and then enter the IP address and subnet mask of the new VLAN logical interface in the IP Address and Subnet Mask fields.
Include this VLAN in an IRB bridge...	If you want the switch port to form part of a bridge with your wireless network, check this box. The other part of the bridge must be configured using the Wireless Application. The IP address and Subnet mask fields under New VLAN are disabled when this box is checked.

Launching the Wireless Application

After completing this LAN configuration, do the following to launch the Wireless Application and complete the bridging configuration.

Step 1 Select **Wireless Application** from the Cisco SDM Tools menu. The Wireless Application opens in a separate browser window.

Step 2 In the Wireless Application, click **Wireless Express Security**, and then click **Bridging** to provide the information to complete the bridging configuration.

IRB Bridge

If you are configuring a VLAN to be part of an IRB bridge, the bridge must be a member of a bridge group.

To create a new bridge group that this interface will be part of, click **Create a new bridge group** and enter a value in the range 1 through 255.

To have this VLAN be a member of an existing bridge group, click **Join an existing bridge group**, and select a bridge group.

Note When you complete the bridge configuration in the Wireless Application, you must use the same bridge group number entered in this screen.

Field Reference

Table 3-8   IP Address and Subnet Mask

Element	Description
Create a new bridge group	To create a new bridge group that this interface will be part of, click **Create a new bridge group** and enter a value in the range 1 through 255.
Join an existing bridge group	To have this VLAN be a member of an existing bridge group, click **Join an existing bridge group**, and select a bridge group.

BVI Configuration

Assign an IP address and subnet mask to the BVI interface. If you selected an existing bridge group in the previous screen, the IP address and subnet mask will appear in this screen. You can change it, or leave the values unchanged**.**

Field Reference

Table 3-9   BVI Configuration

Element	Description
IP Address	Enter the IP address for the interface in dotted decimal format. Your network administrator should determine the IP addresses of LAN interfaces. For more information, see IP Addresses and Subnet Masks.
Net Mask	Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and host portions of the address.
Net Bits	Alternatively, select the number of network bits. This value is used to calculate the subnet mask. Your network administrator can tell you the number of network bits to enter.

DHCP Pool for BVI

When you configure the router as a DHCP server, you can create a pool of IP addresses that clients on the network can use. When a client logs off the network, the address it was using is returned to the pool for use by another host.

Field Reference

Table 3-10   DHCP Pool for BVI

Element	Description
DHCP Server Configuration	If you want to have the router function as a DHCP server, check **DHCP Server Configuration**.
Start IP	Enter the starting IP address for the pool. Be sure to specify IP addresses in the same subnet as the IP address you gave the interface. For example, If you gave the interface an IP address of 10.10.22.1, with a subnet mask of 255.255.255.0, you have over 250 addresses available for the pool, and you might specify a start IP Address of 10.10.22.2.
End IP	Enter the ending IP address for the pool. Using the above example, the end IP address would be 10.10.22.254.

IRB for Ethernet

If your router has a wireless interface, you can use Integrated Routing and Bridging to have this interface form part of a bridge to the wireless LAN, and enable traffic destined for the wireless network to be routed through this interface. Click **Yes** if you want to configure this Layer 3 interface for Integrated Routing and Bridging.

If you do not want this interface to be used in bridge to the wireless interface, click **No**. You will still be able to configure it as a regular routing interface.

Layer 3 Ethernet Configuration

Cisco SDM supports Layer 3 Ethernet configuration on routers with installed 3750 switch modules. You can create VLAN configurations and designate router Ethernet interfaces as DHCP servers.

802.1Q Configuration

You can configure a VLAN that does not use the 802.1Q encapsulation protocol used for trunking connections. Provide a VLAN ID number, and check **Native VLAN** if you do not want the VLAN to use 802.1Q tagging.

If you want to use the 802.1Q tagging, leave the Native VLAN box unchecked.

Field Reference

Table 3-11   IP Address and Subnet Mask

Element	Description
VLAN ID (1-4094)	Enter a VLAN ID number from 1 to 4094. Cisco SDM displays a message telling you to enter a different VLAN ID if the ID that you enter is already in use.
Native VLAN	If you do not want the VLAN to use 802.1Q tagging, check **Native VLAN**. If you want the VLAN to use 802.1Q tagging, leave this box unchecked.

Trunking or Routing Configuration

You can configure Layer 3 Ethernet interfaces for 802.1Q trunking or for basic routing. If you configure the interface for 802.1Q trunking, you can configure VLANs on the interface, and you can configure a native VLAN that does not use the 802.1q encapsulation protocol. I f you configure the interface for routing, you cannot configure subinterfraces or additional VLANs on the interface.

Configure Switch Device Module

If you are configuring a Gigabit Ethernet interface for routing, you can provide information about the switch module in this window. It is not required that you provide this information.

You can provide an IP address and subnet mask for the switch module, and login credentials required to log on to the the switch module interface.

Configure Gigabit Ethernet Interface

Provide IP address and subnet mask information for Gigabit Ethernet interfaces in this window. For more information on IP addresses and subnet masks, see LAN Wizard: IP Address and Subnet Mask.

Field Reference

Table 3-12   IP Address and Subnet Mask

Element	Description
IP Address of Physical Interface	Enter the IP address and subnet mask for the physical Gigabit Ethernet interface in these fields.
IP Address of VLAN Subinterface	Provide the IP address and subnet mask for the VLAN subinterface that you want to create on the physical interface. These fields appear if you are configuring this interface for routing. These fields do not appear if you are configuring this interface for Integrated Routing and Bridging (IRB).

Summary

This window provides a summary of the configuration changes that you made for the interface you selected.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. Although the changes take effect immediately, they will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the User Preferences window, the Deliver window appears. In this window you can view the CLI commands that you are delivering to the router.

Summary

802.1x Authentication

802.1x authentication allows a remote Cisco IOS router to connect authenticated VPN users to a secure network through a VPN tunnel that is up at all times. The Cisco IOS router will authenticate users through a RADIUS server on the secure network.

802.1x authentication is applied to switch ports or Ethernet (routed) ports, but not to both types of interfaces. If 802.1x authentication is applied to an Ethernet port, non-authenticated users can be routed outside the VPN tunnel to the Internet.

802.1x authentication is configured on interfaces by using the LAN wizard. However, before you can enable 802.1x on any interface, AAA must be enabled on your Cisco IOS router. If you attempt to use the LAN wizard before AAA is enabled, a window appears asking if you want to enable AAA. If you choose to enable AAA, then the 802.1x configuration screens will appear as part of the LAN wizard. If you choose to *not* enable AAA, then the 802.1x configuration screens will *not* appear.

LAN Wizard: 802.1x Authentication (Switch Ports)

This window allows you to enable 802.1x authentication on the switch port or ports you selected for configuration using the LAN wizard.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the switch port.

Host Mode

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

✎

Note   Ports on Cisco 85x and Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.

Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN form the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN form the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

Advanced Options

This window allows you to change the default values for a number of 802.1x authentication parameters.

Radius Server Timeout

Enter the time, in seconds, that your Cisco IOS router waits before timing out its connection to the RADIUS server. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Reply Timeout

Enter the time, in seconds, that your Cisco IOS router waits for a reply from an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Retries Timeout

Enter the time, in seconds, that your Cisco IOS router retries an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Quiet Period

Enter the time, in seconds, that your Cisco IOS router will wait between the initial connection to a client and when a login request is sent. Values must be in the range of 1–65535 seconds. The default setting is 60 seconds.

Rate Limit Period

Values must be in the range of 1–65535 seconds. However, the default setting is 0 seconds, which turns off **Rate Limit Period**.

Maximum Reauthentication Attempts

Enter the maximum number of times your Cisco IOS router tries to reauthenticate an 802.1x client. Values must be in the range 1–10. The default setting is 2.

Maximum Retries

Enter the maximum number of login requests that can be sent to the client. Values must be in the range 1–10. The default setting is 2.

Reset to Defaults

Click **Reset to Defaults** to reset all advanced options to their default values.

LAN Wizard: RADIUS Servers for 802.1x Authentication

802.1x authentication information is configured and stored in a policy database residing on RADIUS servers running Cisco Secure ACS version 3.3. The router must validate the credentials of 802.1x clients by communicating with a RADIUS server. Use this window to provide the information the router needs to contact one or more RADIUS servers. Each RADIUS server that you specify must have Cisco Secure ACS software version 3.3 installed and configured.

Note   All of your Cisco IOS router interfaces enabled with 802.1x authorization will use the RADIUS servers set up in this window. When you configure a new interface, you will see this screen again. Additions or changes to the RADIUS server information, however, do not have to be made.

Choose the RADIUS client source

Configuring the RADIUS source allows you to specify the source IP address to be sent in RADIUS packets bound for the RADIUS server. If you need more information about an interface, choose the interface and click the **Details** button.

The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco ACS version 3.3 or later.

If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of interface through which the RADIUS packets exit the router.

If you choose an interface, the source IP address in the RADIUS packets will be the address of the interface that you chose as the RADIUS client source.

Note Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.

Details

If you need a quick snapshot of the information about an interface before choosing it, click **Details**. The screen shows you the IP address and subnet mask, the access rules and inspection rules applied to the interface, the IPSec policy and QoS policy applied, and whether there is an Easy VPN configuration on the interface.

Server IP, Timeout, and Parameters Columns

The Server IP, Timeout, and Parameters columns contain the information that the router uses to contact a RADIUS server. If no RADIUS server information is associated with the chosen interface, these columns are blank.

Use for 802.1x Check Box

Check this box if you want to use the listed RADIUS server for 802.1x. The server must have the required 802.1x authorization information configured if 802.1x is used successfully.

Add, Edit, and Ping

To provide information for a RADIUS server, click the **Add** button and enter the information in the screen displayed. Choose a row and click **Edit** to modify the information for a RADIUS server. Choose a row and click **Ping** to test the connection between the router and a RADIUS server.

Note When performing a ping test, enter the IP address of the RADIUS source interface in the source field in the ping dialog. If you chose **Router chooses source**, you need not provide any value in the ping dialog source field.

The **Edit** and **Ping** buttons are disabled when no RADIUS server information is available for the chosen interface.

Edit 802.1x Authentication (Switch Ports)

This window allows you to enable and configure 802.1x authentication parameters.

If a message is displayed indicating that the port is operating in trunk mode instead of the 802.1x authentication parameters, then the switch cannot have 802.1x authentication enabled.

If the 802.1x authentication parameters appear but are disabled, then one of the following is true:

- AAA has not been enabled.

  To enable AAA, go to **Configure > Additional Tasks > AAA**.

- AAA has been enabled, but an 802.1x authentication policy has not been configured.

  To configure an 802.1x authentication policy, go to **Configure > Additional Tasks > AAA > Authentication Policies > 802.1x**.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on this switch port.

Host Mode

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

Note   Ports on Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.

Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN form the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN form the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

LAN Wizard: 802.1x Authentication (VLAN or Ethernet)

This window allows you to enable 802.1x authentication on the Ethernet port you selected for configuration using the LAN wizard. For Cisco 87x routers, this window is available for configuring a VLAN with 802.1x authentication.

Note   Before configuring 802.1x on VLAN, be sure that 802.1x is *not* configured on any VLAN switch ports. Also be sure that the VLAN is configured for DHCP.

Use 802.1x Authentication to separate trusted and untrusted traffic on the interface

Check **Use 802.1x Authentication to separate trusted and untrusted traffic on the interface** to enable 802.1x authentication.

Exception Lists

Click **Exception Lists** to create or edit an exception list. An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel.

Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

802.1x Exception List

An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel. Exempt clients are identified by their MAC addresses.

Add

Click **Add** to open a window where you can add the MAC address of a client. The MAC address must be in the format that matches one of these examples:

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4

Cisco SDM rejects misformatted MAC addresses, except for MAC addresses shorter than the given examples. Shorter MAC addresses will be padded with a "0" (zero) for each missing digit.

Note   Cisco SDM's 802.1x feature does not support the CLI option that associates policies with MAC addresses and will not include in the exception list MAC addresses that have a policy associated with them.

Delete

Click **Delete** to remove a chosen client from the exception list.

802.1x Authentication on Layer 3 Interfaces

This window allows you to configure 802.1x authentication on a Layer 3 Interface. It lists Ethernet ports and VLAN interfaces that have or can be configured with 802.1x authentication, allows you to choose a Virtual Template interface for untrusted clients, and create an exception list for clients to bypass 802.1x authentication.

Note   If policies have been set using the CLI, they will appear as read-only information in this window. In this case, only enabling or disabling 802.1x is allowed in this window.

Prerequisite Tasks

If a prerequisite task appears in the window, it must be completed before 802.1x authentication can be configured. A message explaining the prerequisite task is displayed, along with a link to the window where the task can be completed.

Enable 802.1x Authentication Globally

Check **Enable 802.1x Authentication Globally** to enable 802.1x authentication on all Ethernet ports.

Interfaces Table

The Interfaces table has the following columns:

Interface—Displays the name of the Ethernet or VLAN interface.

802.1x Authentication—Indicates whether 802.1x authentication is enabled for the Ethernet port.

Edit

Click **Edit** to open a window of editable 802.1x authentication parameters. The parameters are the 802.1x authentication settings for the interface chosen in the Interfaces table.

Untrusted User Policy

Choose a Virtual Template interface from the drop-down list. The chosen Virtual Template interface represents the policy applied to clients that fail 802.1x authentication.

Click the **Details** button to see more information about the chosen Virtual Template interface.

Exception List

For more information about the exception list, see 802.1x Exception List.

Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

Apply Changes

Click **Apply Changes** for the changes you made to take effect.

Discard Changes

Click **Discard Changes** to erase the unapplied changes you made.

Edit 802.1x Authentication

This window allows you to enable and change the default values for a number of 802.1x authentication parameters.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the Ethernet port.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click Advanced Options for descriptions of the fields in the Advanced Options box.

How Do I ...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Configure 802.1x Authentication on More Than One Ethernet Port?

Once you configure 802.1x authentication on an interface, the LAN wizard will no longer display any 802.1x options for Ethernet ports because Cisco SDM uses the 802.1x configuration globally.

Note   For configuring switches, the LAN wizard will continue to display the 802.1x options.

If you want to edit the 802.1x authentication configuration on an Ethernet port, go to **Configure > Additional Tasks > 802.1x**.

Configuring WAN Connections

The WAN wizards enable you to configure WAN connections for all Cisco SDM-supported interfaces.

This chapter contains the following sections:

- Configuring an Ethernet WAN Connection
- Configuring a Serial Connection
- Configuring a DSL Connection
- Configuring an ISDN Connection
- Configuring an Aux Backup Connection
- Configuring an Analog Modem Connection
- Configuring a Cable Modem Connection

Configuring an Ethernet WAN Connection

Complete these steps to configure an Ethernet WAN Connection:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4   In the Create Connection tab, click **Ethernet** WAN.

Step 5   Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6   Click **Next** to go to the subsequent screens to configure the connection.

Step 7   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9   To send the configuration to the router, click **Finish**.

The Ethernet WAN Connection Reference describes the screens that Cisco SDM displays.

Ethernet WAN Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- Encapsulation: PPPoE
- IP Address: Ethernet without PPPoE
- IP Address: ATM or Ethernet with PPPoE/PPPoA
- Authentication
- Advanced Options
- Summary

WAN Wizard Interface Welcome Window

This window lists the types of connections you can configure for this interface using Cisco SDM. If you need to configure another type of connection for this interface, you can do so using the CLI.

Select Interface

This window appears if there is more than one interface of the type you selected in the Create Connection window. Choose the interface that you want to use for this connection.

Field Reference

Table 5-1 describes the fields in this screen.

Table 5-1   *Select Interface Fields*

Element	Description
Check Boxes	Check the box next to the interface that you want to use for this connection.
	If you are configuring an Ethernet interface, Cisco SDM inserts the description text $ETH-WAN$ in the configuration file so that it will recognize the interface as a WAN interface in the future.
Enable Dynamic DNS	Click **Enable Dynamic DNS** if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.
	The Enable Dynamic DNS option is not shown for all connection types.

IP Address: Ethernet without PPPoE

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-2 describes the fields in this screen.

Table 5-2   Ethernet without PPPoE IP Address Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
Dynamic (DHCP Client)	If you choose Dynamic, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Encapsulation: PPPoE

This window lets you enable Point-to-Point-Protocol over Ethernet (PPPoE) encapsulation. This is necessary if your service provider or network administrator requires remote routers to communicate using PPPoE.

PPPoE is a protocol used by many asymmetric digital subscriber line (ADSL) service providers. Ask your service provider if PPPoE is used over your connection.

If you choose PPPoE encapsulation, Cisco SDM automatically adds a dialer interface to the configuration, and this is shown in the Summary window.

Field Reference

Table 5-3 describes the fields in this screen.

Table 5-3   PPoE Encapsulation Fields

Element	Description
Enable PPPoE Encapsulation	If your service provider requires that the router use PPPoE, check this box to enable PPPoE encapsulation. Uncheck this box if your service provider does not use PPPoE. This check box will not be available if your router is running a version of Cisco IOS that does not support PPPoE encapsulation.

Summary

This screen displays a summary of the WAN link that you configured. You can review this information, and if you need to change anything, you can click the Back button to return to the screen on which you need to make changes.

Button Reference

Table 5-4 describes the buttons in this screen.

Table 5-4   **WAN Summary Buttons**

Element	Description
Test the connectivity after configuring	Check this box if you want Cisco SDM to test the connection you have configured after it delivers the commands to the router. Cisco SDM will test the connection and report results in another window.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco SDM Preferences window, the Deliver window appears. In this window, you can view the CLI commands that you are delivering to the router.

Advanced Options

There are two advanced options available, based on the router's configuration: Default static route, and Port Address Translation (PAT). If the Static Route option is not visible in the window, a static route has already been configured on the router. If the PAT option is not visible, PAT has already been configured on an interface.

Field Reference

Table 5-5 describes the fields in this screen.

Table 5-5   Advanced Options Fields

Element	Description
Default Static Route	Check this box if you want to configure a static route to the outside interface to which outgoing traffic will be routed. If a static route has already been configured on this router, this box does not appear.
Next Hop Address	If your service provider has given you a next-hop IP address to use, enter the IP address in this field. If you leave this field blank, Cisco SDM will use the WAN interface that you are configuring as the next-hop interface.
Port Address Translation	If devices on the LAN have private addresses, you can allow them to share a single public IP address. You can ensure that traffic goes to its proper destination by using PAT, which represents hosts on a LAN with a single IP address and uses different port numbers to distinguish the hosts. If PAT has already been configured on an interface, the PAT option will not be visible.
Inside Interface to be Translated	Choose the inside interface connected to the network whose host IP addresses you want to be translated.

Configuring a Serial Connection

Complete these steps to configure a Serial connection:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4   In the Create Connection tab, click **Serial**.

Step 5   Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6   Click **Next** to go to the subsequent screens to configure the connection.

Step 7   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9   To send the configuration to the router, click **Finish**.

The Serial Connection Reference describes the screens that Cisco SDM displays.

Serial Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- IP Address: Serial with Point-to-Point Protocol
- IP Address: Serial with HDLC or Frame Relay
- Authentication
- Configure LMI and DLCI
- Configure Clock Settings
- Advanced Options
- Summary

IP Address: Serial with Point-to-Point Protocol

Choose the method that the point-to-point interface will use to obtain an IP address.

Field Reference

Table 5-6 describes the fields in this screen.

Table 5-6   Serial Connection with Point-to-Point Protocol

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Easy IP (IP Negotiated)	Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

IP Address: Serial with HDLC or Frame Relay

Choose the method that the WAN interface will use to obtain an IP address. If Frame Relay encapsulation is used, Cisco SDM creates a subinterface, and the IP address is assigned to the subinterface Cisco SDM creates.

Field Reference

Table 5-7 describes the fields in this screen.

Table 5-7   Serial Connection with HDLC or Frame Relay Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Table 5-7   Serial Connection with HDLC or Frame Relay Fields

Element	Description
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Authentication

This page is displayed if you enabled or are configuring:

- PPP for a serial connection

- PPPoE or PPPoA encapsulation for an ATM connection

- PPPoE or PPPoA encapsulation for an Ethernet connection

- An ISDN BRI or analog modem connection

Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

Field Reference

Table 5-8 describes the fields in this screen.

Table 5-8   *Authentication Fields*

Element	Description
Authentication Type	Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes: the router will attempt both types of authentication, and one attempt will succeed.
	CHAP authentication is more secure than PAP authentication.
Username	The username is given to you by your Internet service provider or network administrator and is used as the username for CHAP or PAP authentication.
Password	Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password cisco is not the same as Cisco.
Confirm Password	Reenter the same password that you entered in the previous box.

Configure LMI and DLCI

If you are configuring a connection with Frame Relay encapsulation, you must specify the protocol used to monitor the connection, called the Local Management Identifier (LMI), and provide a unique identifier for this particular connection, called a data link connection identifier (DLCI).

Field Reference

Table 5-9 describes the fields in this screen.

Table 5-9   *LMI and DLCI Fields*

Element	Description
LMI Type	
ANSI	Annex D defined by American National Standards Institute (ANSI) standard T1.617.

Table 5-9　　　*LMI and DLCI Fields*

Element	Description
Cisco	LMI type defined jointly by Cisco Systems and three other companies.
ITU-T Q.933	ITU-T Q.933 Annex A.
Autosense	The default. This setting allows the router to detect which LMI type is being used by communicating with the switch and to then use that type. If **autosense** fails, the router will use the Cisco LMI type.
DLCI	Enter the DLCI in this field. This number must be unique among all DLCIs used on this interface.
Use IETF Frame Relay Encapsulation	Internet Engineering Task Force (IETF) encapsulation. This option is used with connecting to non-Cisco routers. Check this box if you are connecting to a non-Cisco router on this interface.

Configure Clock Settings

The Clock Settings window is available when you are configuring a T1 or E1 link. The default Frame Relay clock settings are shown in this page. You should not change them unless you know you have different requirements.

Field Reference

Table 5-10 describes the fields in this screen.

Table 5-10　　　*Clock Settings Fields*

Element	Description
Clock Source	Internal specifies that the clock be generated internally. Line specifies that the clock source be taken from the network. The clock synchronizes data transmission. The default is **line**.
T1 Framing	This field configures the T1 or E1 link for operation with D4 Super Frame (sf) or Extended Superframe (esf). The default is **esf**.

Table 5-10   Clock Settings Fields

Element	Description
Line Code	This field configures the router for operation on binary 8-zeros substitution (B8ZS) or alternate mark inversion (AMI) T1 lines. The b8zs setting ensures density on a T1 or E1 line by substituting intentional bipolar violations in bit positions 4 and 7 for a sequence of eight zero bits. When the router is configured with the AMI setting, you must use the data-coding inverted setting to ensure density on the T1 line. The default is **b8zs**.
Data Coding	Click **inverted** if you know that user data is inverted on this link, or if the Line Code field is set to AMI. Otherwise leave this set to the default value **normal**. Data inversion is used with bit-oriented protocols such as HDLC, PPP, and Link Access Procedure, Balanced (LAPB) to ensure density on a T1 line with AMI encoding. These bit-oriented protocols perform "zero insertions" after every five "one" bits in the data stream. This has the effect of ensuring at least one zero in every eight bits. If the data stream is then inverted, it ensures that at least one out of every eight bits is a one. Cisco SDM will set data coding to inverted if the line code is AMI and there are no time slots configured for 56 kbps. If you do not want to use inverted data coding with the AMI line code, you must use the CLI to configure all time slots to 56 kbps.
Facilities Data Link (FDL)	This field configures the router behavior on the Facilities Data Link (FDL) of the Extended Superframe. When configured with **att**, the router implements AT&T TR 54016. When configured with **ansi**, it implements ANSI T1.403. When you choose both, the router implements both **att** and **ansi** choices. When you choose none, the router ignores the FDL. The default is **none. If T1 or E1 framing is set to sf,** Cisco SDM will set FDL to **none** and make this field read-only.
Line Build Out (LBO)	This field is used to configure the line build out (LBO) of the T1 link. The LBO decreases the transmit strength of the signal by –7.5 or –15 decibels. It is not likely to be needed on actual T1 or E1 lines. The default is **none**.

Table 5-10   Clock Settings Fields

Element	Description
Remote Loopback Requests	This field specifies whether the router will go into loopback mode when a loopback code is received on the line. Choosing **full** causes the router to accept full loopbacks, while choosing **payload-v54** will cause the router to choose payload loopbacks.
Enable Generation/Detection of Remote Alarms	Check this box if you want the router T1 link to generate remote alarms (yellow alarms) and to detect remote alarms being sent from the peer on the other end of the link.
	The remote alarm is transmitted by a router when it detects an alarm condition: either a red alarm (loss of signal) or a blue alarm (unframed 1s). The receiving channel service unit/data service unit (CSU/DSU) then knows that there is an error condition on the line.
	This setting should only be used when T1 framing is set to **esf**.

Configuring a DSL Connection

Complete these steps to configure an ADSL, or G.SHDSL connection:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit** > **Preferences** > **Preview commands before delivering to router**.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4   The Create Connection tab displays the available DSL connection types, for example, ADSL (PPPoE or RFC 1483 routing or PPPoA). Choose an available connection type.

Step 5   Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6   Click **Next** to go to the subsequent screens to configure the connection.

Step 7   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9   To send the configuration to the router, click **Finish**.

The DSL Connection Reference describes the screens that Cisco SDM displays.

DSL Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- Encapsulation: PPPoE
- Encapsulation Autodetect
- IP Address: ATM or Ethernet with PPPoE/PPPoA
- IP Address: ATM with RFC 1483 Routing
- Authentication
- Advanced Options
- PVC
- Summary

IP Address: ATM or Ethernet with PPPoE/PPPoA

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-11 describes the fields in this screen.

Table 5-11   ATM or Ethernet with PPPoE or PPPoA

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided.
Dynamic (DHCP Client)	If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Easy IP (IP Negotiated)	Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

IP Address: ATM with RFC 1483 Routing

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-12 describes the fields in this screen.

Table 5-12   *ATM with RFC 1483 Routing*

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
Dynamic (DHCP Client)	If you choose Dynamic, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
IP Unnumbered	Click **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Encapsulation Autodetect

In this window, choose the type of encapsulation that the WAN link will use. Ask your service provider or network administrator which type of encapsulation is used for this link. The interface type determines the types of encapsulation available.

Field Reference

Table 5-13 describes the fields in this screen.

Table 5-13   Encapsulation Fields

Element	Description
Autodetect	Click **Autodetect** to have Cisco SDM discover the encapsulation type. If Cisco SDM succeeds, it will automatically supply the encapsulation type and other configuration parameters it discovers. **Note** Cisco SDM supports autodetect on SB106, SB107, Cisco 836, and Cisco 837 routers. However if you are configuring a Cisco 837 router and the router is running Cisco IOS Release 12.3(8)T or 12.3(8.3)T, the autodetect feature is not supported.
Encapsulations Available for ADSL, G.SHDSL, or ADSL over ISDN	
PPPoE	Provides Point-to-Point Protocol over Ethernet encapsulation. This option is available when you have selected an Ethernet interface or an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoE over an ATM interface. The PPPoE radio button will be disabled if your router is running a version of Cisco IOS that does not support PPPoE encapsulation.
PPPoA	Point-to-Point protocol over ATM. This option is available when you have selected an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoA over an ATM interface. The PPPoA radio button will be disabled if your router is running a version of Cisco IOS that does not support PPPoA encapsulation.
RFC 1483 routing with AAL5-SNAP	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. This subinterface will be visible in the Summary window.
RFC 1483 routing with AAL5-MUX	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. This subinterface will be visible in the Summary window.

Table 5-13   Encapsulation Fields

Element	Description
Encapsulations Available for Serial Interfaces	
Frame Relay	Provides Frame Relay encapsulation. This option is available when you have selected a serial interface. A serial subinterface will be created when you create a Frame Relay connection. This subinterface will be visible in the Summary window.
	Note If a Frame Relay serial connection has been added to an interface, only Frame Relay encapsulation will be enabled in this window when subsequent serial connections are configured on the same interface.
Point-to-Point Protocol	Provides PPP encapsulation. This option is available when you have selected a serial interface.
High Level Data Link Control	Provides HDLC encapsulation. This option is available when you have selected a serial interface.

PVC

ATM routing uses a two-layer hierarchical scheme, virtual paths and virtual channels, denoted by the virtual path identifier (VPI) and virtual channel identifier (VCI), respectively. A particular virtual path may carry a number of different virtual channels corresponding to individual connections. When switching is performed based on the VPI, all cells on that particular virtual path are switched regardless of the VCI. An ATM switch may route according to VCI, VPI, or both VCI and VPI.

Field Reference

Table 5-14 describes the fields in this screen.

Table 5-14   PVC Fields

Element	Description
VPI	Enter the VPI value obtained from your service provider or system administrator. The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Enter the VPI value given to you by your service provider.
VCI	Enter the VCI value obtained from your service provider or system administrator. The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Enter the VCI value given to you by your service provider.

Cisco IOS Default Values

The values shown in the following table are Cisco IOS defaults. Cisco SDM will not overwrite these values if they have been changed during a prior configuration, but if your router has not been previously configured, these are the values that will be used

Connection Type	Parameter	Value
ADSL	• Operating mode	• Auto
G.SHDSL	• Operating mode	• Annex A (United States)
	• Line rate	• Auto
	• Equipment type	• CPE
ADSL over ISDN	• Operating mode	• Auto

Configuring an ISDN Connection

Complete these steps to configure an ISDN connection:

Step 1 If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**.

Step 2 In the Cisco SDM toolbar, click **Configure**.

Step 3 In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4 In the Create Connection tab, click **ISDN (PPP)**.

Step 5 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6 Click **Next** to go to the subsequent screens to configure the connection.

Step 7 Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9 To send the configuration to the router, click **Finish**.

The ISDN Connection Reference describes the screens that Cisco SDM displays.

ISDN Connection Reference

- ISDN Wizard Welcome Window
- Select Interface
- IP Address: ISDN BRI or Analog Modem
- Switch Type and SPIDs
- Authentication

- Advanced Options
- Dial String
- Summary

ISDN Wizard Welcome Window

PPP is the only type of encoding supported over an ISDN BRI by Cisco SDM.

IP Address: ISDN BRI or Analog Modem

Choose the method that the ISDN BRI or analog modem interface will use to obtain an IP address.

Field Reference

Table 5-15 describes the fields in this screen.

Table 5-15   IP Address for ISDN BRI or Analog Modem Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then, choose the interface that has the IP address that you want the interface that you are configuring to use.
Easy IP (IP Negotiated)	Choose **IP Negotiated** if the interface will obtain an IP address from your ISP through PPP/IPCP address negotiation whenever a connection is made.
Dynamic DNS	Choose **Dynamic DNS** if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Switch Type and SPIDs

ISDN BRI connections require identification of the ISDN switch type, and in some cases, identification of the B channels using service profile ID (SPID) numbers. This information will be provided to you by your service provider.

Field Reference

Table 5-16 describes the fields in this screen.

Table 5-16   Switch Type and SPIDs Fields

Element	Description
ISDN Switch Type	Choose the ISDN switch type. Contact your ISDN service provider for the switch type for your connection.
	Cisco SDM supports these BRI switch types:
	–
	• For North America:
	– basic-5ess—Lucent (AT&T) basic rate 5ESS switch
	– basic-dms100—Northern Telecom DMS-100 basic rate switch
	– basic-ni—National ISDN switches
	• For Australia, Europe, and the UK:
	– basic-1tr6—German 1TR6 ISDN switch
	– basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
	– vn3—French ISDN BRI switches
	• For Japan:
	– ntt—Japanese NTT ISDN switches

Table 5-16   Switch Type and SPIDs Fields

Element	Description
	• For voice or PBX systems: – basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931
I have SPIDS	Check this check box if your service provider requires SPIDs. Some service providers use SPIDs to define the services that are subscribed to by an ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when the device accesses the switch to initialize the connection. Currently, only the DMS-100 and NI switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, but we recommend that you set up the ISDN service without SPIDs. In addition, SPIDs have significance only at the local access ISDN interface. Remote routers never receive the SPID. A SPID is usually a 7-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.
Spid 1	Enter the SPID for the first BRI B channel provided to you by your ISP.
Spid 2	Enter the SPID for the second BRI B channel provided to you by your ISP.

Dial String

Enter the phone number of the remote end of the ISDN BRI or analog modem connection. This is the phone number that the ISDN BRI or analog modem interface will dial whenever a connection is made. The dial string is provided to you by your service provider.

Configuring an Aux Backup Connection

Complete these steps to configure an Aux Backup connection:

Step 1 If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences** > **Preview commands before delivering to router**.

Step 2 In the Cisco SDM toolbar, click **Configure**.

Step 3 In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4 In the Create Connection tab, click **Aux Backup**.

Step 5 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6 Click **Next** to go to the subsequent screens to configure the connection.

Step 7 Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9 To send the configuration to the router, click **Finish**.

The Aux Backup Connection Reference describes the screens that Cisco SDM displays.

Aux Backup Connection Reference

- Aux Backup Welcome Window
- Backup Configuration
- Backup Configuration: Primary Interface and Next Hop IP Addresses
- Backup Configuration: Hostname or IP Address to Be Tracked

• Summary

Aux Backup Welcome Window

The option to configure the AUX port as a dial-up connection only appears for the Cisco 831 and 837 routers.

The Aux dial-backup radio button is disabled if any of the following conditions exist:

• More than one default route exists.

• One default route exists and it is configured with an interface other than the primary WAN interface.

The Aux dial-backup option is not shown if any of the following conditions exist:

• The router is not using a Cisco IOS image that supports the Aux dial-backup feature.

• A primary WAN interface is not configured.

• The asynchronous interface is already configured.

• The asynchronous interface is not configurable by Cisco SDM because of the presence of unsupported Cisco IOS commands in the existing configuration.

Backup Configuration

ISDN BRI and analog modem interfaces can be configured to work as backup interfaces to other, primary interfaces. In that case, an ISDN or analog modem connection will be made only if the primary interface goes down for some reason. If the primary interface and connection go down, the ISDN or analog modem interface will immediately dial out and try to establish a connection so that network services are not lost.

Choose whether this ISDN BRI or analog modem connection should act as a backup connection.

Field Reference

Table 5-17 describes the fields in this screen.

Table 5-17   Backup Configuration Fields

Element	Description
Configure this connection as backup	Check this option to designate this interface as backup.
Do not configure this connection as backup.	Check this option if you do not want to designate this interface as backup.

Prerequisites

Note the following prerequisites:

- The primary interface must be configured for site-to-site VPN.
- The Cisco IOS image on your router must support the SAA ICMP Echo Enhancement feature.

Backup Configuration: Primary Interface and Next Hop IP Addresses

In order for the ISDN BRI or analog modem connection to act as a backup connection, it must be associated with another interface on the router that will act as the primary connection. The ISDN BRI or analog modem connection will be made only if the connection on the primary interface goes down.

Field Reference

Table 5-18 describes the fields in this screen.

Table 5-18   Hostname or IP Address to Be Tracked Fields

Element	Description
Primary Interface	Enter the IP address or hostname of the destination host to which connectivity will be tracked. Please specify an infrequently contacted destination as the site to be tracked.

Table 5-18   Hostname or IP Address to Be Tracked Fields

Element	Description
Primary Next Hop IP Address	Choose the router interface that will maintain the primary connection.
Backup Next Hop IP Address	This field is optional. Enter the IP address to which the backup interface will connect when it is active, known as the *next hop IP address*.

Backup Configuration: Hostname or IP Address to Be Tracked

This screen lets you identify a specific host to which connectivity must be maintained. The router will track connectivity to that host, and if the router discovers that connectivity has been lost by the primary interface, a backup connection will be initiated over the ISDN BRI or analog modem interface.

Field Reference

Table 5-19 describes the fields in this screen.

Table 5-19   Hostname or IP Address to Be Tracked Fields

Element	Description
IP Address to Be Tracked	Enter the IP address or hostname of the destination host to which connectivity will be tracked. Please specify an infrequently contacted destination as the site to be tracked.

Configuring an Analog Modem Connection

Complete these steps to configure an Analog Modem connection:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4   In the Create Connection tab, click **Analog Modem**.

Step 5   Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6   Click **Next** to go to the subsequent screens to configure the connection.

Step 7   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9   To send the configuration to the router, click **Finish**.

The Analog Modem Connection Reference describes the screens that Cisco SDM displays.

Analog Modem Connection Reference

- Analog Modem Welcome
- IP Address: ISDN BRI or Analog Modem
- Authentication
- Dial String
- Summary

Analog Modem Welcome

This screen describes the tasks you will perform to configure an analog modem connection. PPP is the only type of encoding supported over an analog modem connection by Cisco SDM.

Configuring a Cable Modem Connection

Complete these steps to configure a Cable Modem connection:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Interfaces and Connections**.

Step 4   In the Create Connection tab, click **Cable Modem**.

Step 5   Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 6   Click **Next** to go to the subsequent screens to configure the connection.

Step 7   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 9   To send the configuration to the router, click **Finish**.

The Cable Modem Connection Reference describes the screens that Cisco SDM displays.

Cable Modem Connection Reference

- Cable Modem Connection Wizard Welcome
- Select Interface
- Advanced Options
- Summary

Cable Modem Connection Wizard Welcome

The Welcome screen indicates that you are using the cable modem connection wizard, and describes the tasks you perform when you configure a Cable Modem connection.

Click **Next** to begin configuring the connection.

Select Interface

Select the cable modem interface to configure in this screen. The interface that you select will be configured as a DHCP client.

Field Reference

Table 5-20 describes the fields in this screen.

Table 5-20   Select Interface

Element	Description
Select an interface for the WAN connection	Choose the cable modem interface that you want to configure.
Enable Dynamic DNS	Check **Enable Dynamic DNS** if you want to update your DNS servers automatically whenever the WAN interface IP address changes.
Dynamic DNS	Click the Dynamic DNS button to configure a dynamic DNS method. See Add or Edit Dynamic DNS Method for more information.

Summary

The Summary screen shows the configuration you are sending to the router. Cisco SDM configures a cable modem connection as a DHCP client. The following lines show cable modem connection with no NAT or static route configuration

```
Selected Interface: Cable Modem 0/1/0
IP Address: Dynamic (DHCP Client)
```

Field Reference

Table 5-21 describes the buttons in this screen.

Table 5-21   Summary Buttons

Element	Description
Test the connectivity after configuring	Check this box if you want Cisco SDM to test the connection you have configured after it delivers the commands to the router. Cisco SDM will test the connection and report results in another window.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco SDM Preferences window, the Deliver window appears. In this window, you can view the CLI commands that you are delivering to the router.

C H A P T E R 6

Edit Interface/Connection

This window displays the router's interfaces and connections. The window also enables you to add, edit, and delete connections, and to enable or disable connections.

Add

When you choose an unconfigured physical interface and click **Add**, the menu contains choices for adding a connection on that interface. Click **Add** to create a new loopback or tunnel interface. If the Cisco IOS image on the router supports Virtual Template Interfaces (VTI), the context menu contains an option to add a VTI. If there are switch ports present on the router, you can add a new VLAN.

If you want to reconfigure an interface, and see no choices except Loopback and Tunnel when you click **Add**, choose the interface and click **Delete**. All the types of connections available for that kind of interface will appear in the Add menu. Click **Available Interface Configurations** to see what configurations are available for an interface.

Edit

When you choose an interface and click **Edit**, a dialog appears. If the interface is a supported and configured interface and is not a switch port, the dialog will have the following tabs:

- Connection
- Association tab
- NAT tab

- Application Service
- General tab

If the interface is not supported, the dialog will *not* have a Connection tab. If you choose a switch port, the Edit Switch Port dialog appears. The Edit button will be disabled if the interface is supported and unconfigured.

Delete

Choosing a connection and clicking **Delete** displays a dialog box informing you of the associations this connection has and asking you if you want to remove the associations along with the connection. You can delete just the connection, or the connection and all of its associations.

Summary

Clicking the Summary button hides the details about the connection, restricting the information to the IP address, Type, Slot, Status, and Description.

Details

Clicking **Details** displays the Details About Interface area, described next. Details about the interface are shown by default.

Enable or Disable

When the chosen interface or connection is down, this appears as the **Enable** button. Click the **Enable** button to bring up the chosen interface or connection. When the chosen interface or connection is up, this appears as the **Disable** button. Click the **Disable** button to administratively shut down the interface or connection. This button cannot be used with an interface whose configuration was not delivered to the router.

Test Connection

Click to test the chosen connection. A dialog appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps you need to take to correct the problem.

Interface List

The interface list displays the physical interfaces and the logical connections to which they are configured.

Interfaces

This column lists the physical and logical interfaces by name. If a logical interface is configured for a physical interface, the logical interface is shown under the physical interface.

If Cisco SDM is running on a Cisco 7000 family router, you will be able to create a connection only on Ethernet and Fast Ethernet interfaces.

IP Address

This column can contain the following types of IP addresses:

- The configured IP address of the interface.

- DHCP Client—The interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.

- IP address negotiated—The interface receives an IP address through negotiation with the remote device.

- IP unnumbered—The router will use one of a pool of IP addresses supplied by your service provider for your router, and for the devices on the LAN.

- Not Applicable—The interface type cannot be assigned an IP address.

Type

The Type column displays the interface type, such as Ethernet, serial, or ATM.

Slot

The number of the physical slot in the router that the interface is installed in. If Cisco SDM is running on a Cisco 1710 router, the slot field is empty.

Status

This column shows whether this interface is up or down. The green icon with the upward-pointing arrowhead indicates the interface is up. The red icon with the downward-pointing arrowhead indicates that the interface is down.

Description

This column contains any descriptions provided for this connection.

Details About Interface

This area of the window displays association and, if applicable, connection details about the interface chosen in the interface list. Association details include such information as Network Address Translation (NAT), access, and inspection rules, IPsec policies, and Easy VPN configurations. Connection details include IP address, encapsulation type, and DHCP options.

Item Name

The name of the configuration item, such as IP address/Subnet mask, or IPsec policy. The actual items listed in this column depend on the type of interface chosen.

Item Value

If the named item has a configured value, it is displayed in this column.

Why Are Some Interfaces or Connections Read-Only?

There are many conditions that can prevent Cisco SDM from modifying a previously configured interface or subinterface.

- For reasons why a previously configured serial interface or subinterface may appear as read-only in the interface list, see the help topic Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only.

- For reasons why a previously configured ATM interface or subinterface may appear as read-only in the interface list, see the help topic Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only.

- For reasons why a previously configured Ethernet LAN or WAN interface may appear as read-only in the interface list, see the help topic Reasons Why an Ethernet Interface Configuration May Be Read-Only.

- For reasons why a previously configured ISDN BRI interface may appear as read-only in the interface list, see the help topic Reasons Why an ISDN BRI Interface Configuration May Be Read-Only.

Connection: Ethernet for IRB

This dialog box contains the following fields if you chose **Ethernet for IRB** in the Configure list.

Current Bridge Group/Associated BVI

These read-only fields contain the current bridge group value and the current Bridge-Group Virtual Interface (BVI) name.

Create a new Bridge Group/Join an existing Bridge Group

Choose whether you want to make this interface a member of a new bridge group, or if you want to join an existing bridge group. If you want to create a new bridge group, enter a number in the range 1 to 255. If you want to have the interface join an existing bridge group, choose the BVI interface that is already a member of that group.

IP Address

Enter the IP address and subnet mask in the fields provided.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet for Routing

This dialog box contains the following fields if you chose **Ethernet for Routing** in the Configure list.

IP Address

Enter an IP address and subnet mask in the IP Address fields. This address will be the source IP address for traffic originating from this interface, and the destination IP address for traffic destined for hosts connected to this interface.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of one DHCP relay or one DHCP server per subnetwork.

Note   If the router was configured to be a DHCP relay and to have more than one remote DHCP server IP address, these fields are disabled.

IP Address of Remote DHCP Server

Enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Existing Dynamic DNS Methods

This window allows you to choose a dynamic DNS method to associate with a WAN interface.

The list of existing dynamic DNS methods shows each method's name and associated parameters. Choose a method from the list, and then click **OK** to associate it to the WAN interface.

To add, edit, or delete dynamic DNS methods, go to **Configure > Additional Tasks > Dynamic DNS Methods**.

Add Dynamic DNS Method

This window allows you to add a dynamic DNS method. Choose the type of method, HTTP or IETF, and configure it.

HTTP

HTTP is a dynamic DNS method that updates a DNS service provider with changes to the associated interface's IP address.

Server

If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.

Username

If using HTTP, enter a username for accessing the DNS service provider.

Password

If using HTTP, enter a password for accessing the DNS service provider.

IETF

IETF is a dynamic DNS method that updates a DNS server with changes to the associated interface's IP address.

DNS Server

If using IETF, and no DNS server is configured for the router in **Configure > Additional Tasks > DNS**, then enter the IP address of your DNS server.

Hostname

Enter a hostname if one is not configured in **Configure > Additional Tasks > Router Properties > Edit > Host**, or if you want to override the configured hostname. When updating the interface IP address, the dynamic DNS method sends the hostname along with the interface's new IP address.

Domain Name

Enter a domain name if one is not configured in **Configure > Additional Tasks > Router Properties > Edit > Domain**, or if you want to override the configured domain name. When updating the interface IP address, the dynamic DNS method sends the domain name along with the interface's new IP address.

Wireless

If the router has a wireless interface, you can launch the wireless application from this tab. You can also launch the wireless application from the Tools menu by choosing **Tools** > **Wireless Application**.

Association

Use this window to view, create, edit, or delete associations between interfaces and rules or VPN connections.

Interface

The name of the interface you selected in the Interfaces and Connections window.

Zone

If this interface is a member of a security zone, the name of the zone is displayed in this field. If you want to include this interface in a security zone, click the button to the right of the field, choose **Select a Zone**, and specify the zone in the displayed dialog. If you need to create a new zone, choose **Create a Zone**, enter a name for the zone in the displayed dialog, and click OK. The name of the zone you created appears in the zone field.

Access Rule

The names or numbers of any access rules associated with this interface. Access rules permit or deny traffic that matches the IP address and service criteria specified in the rule.

Inbound

The name or number of an access rule applied to inbound traffic on this interface. If you want to apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to inbound traffic on an interface, the rule filters traffic before it enters the router. Any packet that the rule does not permit is dropped and will not be routed to another interface. When you apply a rule to the inbound

direction on an interface, you are not only preventing it from entering a trusted network connected to the router, you are also preventing it from being routed anywhere else by the local router.

Outbound

The name or number of an access rule applied to outbound traffic on this interface. If you want to apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to outbound traffic on an interface, the rule filters traffic after it enters the router and before it exits the interface. Any packet that the rule does not permit is dropped before it leaves the interface.

Inspect Rule

The names of inspection rules associated with this interface. Inspection rules create temporary holes in firewalls so that hosts inside the firewall that started sessions of a certain type can receive return traffic of the same type.

Inbound

The name or number of an inspection rule applied to inbound traffic on this interface. If you want to apply an inbound rule, click the **Inbound** drop-down menu and choose a rule.

Outbound

The name or number of an inspection rule applied to outbound traffic on this interface. If you want to apply an outbound rule, click the **Outbound** drop-down menu and choose a rule.

VPN

VPNs protect traffic that may flow over lines that your organization does not control. You can use the chosen interface in a VPN by associating it with an IPsec policy.

IPsec Policy

The configured IPsec policy associated with this interface. To associate the interface with an IPsec policy, choose the policy from this list.

> ✎
> **Note**   An interface can be associated with only one IPsec policy.

> ✎
> **Note**   To create a GRE-over-IPsec Tunnel, you must first associate the policy with the tunnel interface, and then associate it with the source interface for the tunnel. For example, if you wanted to associate a policy with Tunnel3, whose source interface is Serial0/0, you would first choose Tunnel3 in the Interfaces and Connections window, click **Edit** and associate the policy with it, and then click **OK**. Then you would choose the Serial0/0 interface and associate the same policy with it.

EzVPN

If the interface is used in an Easy VPN connection, the name of the connection is shown here.

> ✎
> **Note**   An interface cannot be used in both a virtual private network (VPN) connection and an Easy VPN connection.

Making Association Changes

When you change the association properties of an interface, the changes are reflected in the lower portion of the Edit Interface/Connection window. For example, if you associate an IPsec policy with the interface, the name of the IPsec policy appears in the lower portion of the window. If you delete an association, the value in the Item Value column changes to <None>.

NAT

If you intend to use this interface in a NAT configuration, you must designate it as either an inside or an outside interface. Choose the traffic direction to which NAT is to be applied. If the interface connects to a LAN that the router serves, choose **Inside**. If it connects to the Internet or to your organization's WAN, choose **Outside**. If you have chosen an interface that cannot be used in a NAT configuration, such as a logical interface, this field is disabled and contains the value Not Supported.

Edit Switch Port

This window lets you edit VLAN information for Ethernet switch ports.

Mode Group

Choose the type of VLAN information you want to be carried across this Ethernet switch port. Choosing **Access** causes the switch port to forward only data destined for the specific VLAN number. Choosing **Trunking** causes the switch port to forward data for all VLANs, including the VLAN data itself. Choose **Trunking** only for "trunking" VLAN ports that connect to other networking devices, such as another switch, that will connect to devices in multiple VLANs.

VLAN

To assign the switch port to a VLAN, enter the VLAN number to which this switch port should belong. If the switch port does not already have a VLAN associated with it, this field will show the default value VLAN 1. To create a new VLAN interface corresponding to a VLAN ID, enter that VLAN ID here and check the **Make VLAN visible to interface list** check box.

Make VLAN visible to interface list Check Box

Check if you want to create a new VLAN with the VLAN ID specified in the VLAN field.

Stacking Partner

Choose a switch module as the stacking partner to use. When a device contains multiple switching modules, these must be stacked before other stacking partners.

Bridge Group Number

If you want this switch port to form part of a bridge to a wireless network, enter the number of an existing bridge group.

Speed

Choose the speed to match the network to which the switch port will be connected. Or choose **auto** to allow for the speed to be automatically set to the optimal value.

Duplex

Choose **full** or **half**, or **auto** to allow for the duplex to be automatically set to match the network to which the switch port will be connected.

If **Speed** is set to **auto**, then **Duplex** is disabled.

Power Inline

The **Power inline** drop-down list appears if the switch port supports an inline power supply. Choose one of the following values:

- **auto**—Automatically detect and power inline devices.

- **never** —Never apply inline power.

Application Service

This window allows you to associate QoS policies and application and protocol monitoring with the chosen interface.

QoS

To associate a QoS policy with the interface in the inbound direction, choose a QoS policy from the **Inbound** drop-down menu.

To associate a QoS policy with the interface in the outbound direction, choose a QoS policy from the **Outbound** drop-down menu.

QoS statistics for the interface can be monitored by going to **Monitor > Traffic Status > QoS**.

Netflow

To associate Netflow statistics monitoring with the interface in the inbound direction, check the **Inbound** check box.

To associate Netflow statistics monitoring with the interface in the outbound direction, check the **Outbound** check box.

Netflow statistics for the interface can be monitored by going to **Monitor > Interface Status**. Netflow top talkers and top protocols can be monitored by going to **Monitor > Traffic Status > Top N Traffic Flows**.

NBAR

To associate Network-based application recognition (NBAR) with the interface, check the **NBAR Protocol** check box.

NBAR statistics for the interface can be monitored by going to **Monitor > Traffic Status > Application/Protocol Traffic**.

General

This window displays general security settings and allows you to enable or disable them by checking or unchecking the check box next to the name and description. If you have allowed the Security Audit feature to disable certain properties and want to reenable them, you can reenable them in this window. The properties listed in this window follow.

Description

In this field you can enter a short description of the interface configuration. This description is visible in the Edit Interfaces and Connections window. A description, such as "Accounting" or "Test Net 5," can help other Cisco SDM users understand the purpose of the configuration.

IP Directed Broadcasts

An IP directed broadcast is a datagram that is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the extremely common and popular "smurf" denial of service attack, and they can also be used in related attacks. In a "smurf" attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send

replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger reply stream, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts drops directed broadcasts that would otherwise be "exploded" into link-layer broadcasts at that interface.

IP Proxy ARP

ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, and a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

IP Route Cache-Flow

This option enables the Cisco IOS Netflow feature. Using Netflow, you can determine packet distribution, protocol distribution, and current flows of data on the router. This information is useful for certain tasks, such as searching for the source of a spoofed IP address attack.

Note   The IP Route Cache-Flow option enables Netflow on both inbound and outbound traffic. To enable Netflow on either inbound traffic *or* outbound traffic, use the Netflow options available on the **Application Service** tab.

IP Redirects

ICMP redirect messages instruct an end node to use a specific router as a part of its path to a particular destination. In a properly functioning IP network, a router sends redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever traverse more than one network hop. However, an attacker may violate these rules. Disabling ICMP redirects has no negative impact on the network and can eliminate redirect attacks.

IP Mask-Reply

ICMP mask reply messages are sent when a network device must know the subnet mask for a particular subnetwork in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

IP Unreachables

ICMP host unreachable messages are sent if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

Select Ethernet Configuration Type

This window is displayed when you click an interface in the Interfaces and Connections window and Cisco SDM cannot determine whether the interface is configured as a LAN interface or as a WAN interface. When you configure an interface using Cisco SDM, you designate it as an inside or outside interface, and Cisco SDM adds a descriptive comment to the configuration file based on your designation. If you configure an interface using the command-line interface (CLI), the configuration will not include this descriptive comment, and Cisco SDM will not have this information.

To Indicate that the Interface is a LAN Interface:

Click **LAN**, and then click **OK**. Cisco SDM adds the comment line $ETH-LAN$ to the interface configuration, and the interface appears in the LAN wizard window with the designation Inside in the Interfaces and Connections window.

To Indicate that the Interface is a WAN Interface:

Click **WAN**, and then click **OK**. Cisco SDM adds the comment line $ETH-WAN$ to the interface configuration, and the interface appears in the WAN wizard window with the designation Outside in the Interfaces and Connections window.

Connection: VLAN

This window lets you configure a VLAN interface.

VLAN ID

Enter the ID number of the new VLAN interface. If you are editing a VLAN interface, you cannot change the VLAN ID.

Native VLAN Check Box

Check if this VLAN is a nontrunking VLAN.

IP Address Fields

IP Address Type

Choose whether this VLAN interface will have a static IP address or no IP address. This field is visible when **VLAN only** is chosen in the Configure As field.

IP Address

Enter the IP address of the VLAN interface.

Subnet Mask

Enter the subnet mask of the VLAN interface, or indicate the number of subnet bits using the scrolling field.

DHCP Relay

Click DHCP Relay for more information.

Subinterfaces List

This window displays the subinterfaces configured for the interface that you chose, and enables you to add, edit, and remove configured subinterfaces. For each configured subinterface, the window displays the Subinterface ID, VLAN ID, IP address and mask, and a description, if one was entered. For example, if the router had the interface FastEthernet1, and the subinterfaces FastEthernet1.3 and FastEthernet1.5 are configured, this window might contain the following display

```
5       56      56.8.1.1/255.255.255.0
3       67      Bridge No. 77
```

In this example, FastEthernet1.5 is configured for routing, and FastEthernet1.3 is configured for IRB.

Note You must choose the physical interface on which the subinterfaces are configured to display this window. For the example described, you would have to choose FastEthernet 1 to display this window. If you chose FastEthernet1.3 or FastEthernet1.5 and clicked edit, you would display the edit dialog with the information for that interface.

Add, Edit, and Delete Buttons

Use these buttons to configure, edit, and remove subinterfaces from the chosen physical interface.

Add or Edit BVI Interface

Add or edit a Bridge Group Virtual Interface (BVI) in this window. If your router has a Dot11Radio interface, a BVI is automatically created when you configure a new bridge group. This is done to support IRB bridging. You can change the IP address and subnet mask in this window.

IP Address/Subnet Mask

Enter the IP address and subnet mask that you want to give the BVI.

Add or Edit Loopback Interface

This window enables you to add a loopback interface to the chosen interface.

IP Address

Choose whether the loopback interface is to have no IP address or a static IP address.

Static IP Address

If you chose **Static IP address**, enter that IP address in this field.

Subnet Mask

Enter the subnet mask in this field, or choose the number of subnet bits from the field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Connection: Virtual Template Interface

You can add or edit a VTI as part of an 802.1x or VPN configuration. When you are editing a VTI, the fields that you can edit appear in a Connection tab.

Interface Type

Choose either **default** or **tunnel**. If you choose tunnel, you must also select a tunnel mode.

IP Address

Choose **Unnumbered**. The VTI uses the IP address of the physical interface that is chosen in the Unnumbered to field.

Unnumbered to

This field appears when you choose **Unnumbered** in the IP Address field. Choose the interface whose IP address you want this VTI to use.

Tunnel Mode

Choose **IPSec-IPv4**.

Connection: Ethernet LAN

Use this window to configure the IP address and DHCP properties of an Ethernet interface that you want to use as a LAN interface.

IP Address

Enter the IP address for this interface. Obtain the IP address value from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and subnet portion of the address.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of 1 DHCP relay or 1 DHCP server per subnetwork.

> **Note**   If the router was configured to be a DHCP relay with more than one remote DHCP server IP address, this button will be disabled.

IP Address of Remote DHCP Server

If you clicked **DHCP Relay**, enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Connection: Ethernet WAN

This window lets you add an Ethernet WAN connection.

Enable PPPoE Encapsulation

Click this option if the connection must use Point-to-Point Protocol over Ethernet (PPPoE) encapsulation. Your service provider can tell you whether the connection uses PPPoE. When you configure a PPPoE connection, a dialer interface is automatically created.

IP Address

Choose one of the following IP address types, and enter the information in the fields displayed. If the Ethernet connection is not using PPPoE, you will see only the Static IP address and Dynamic options.

Static IP Address

If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server from which addresses will be leased.

IP Unnumbered

Choose **IP Unnumbered** if you want the interface to share an IP address that is already assigned to another interface. Then choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Choose Easy IP (IP Negotiated) if the router will obtain an IP address through Point-to-Point Protocol/IP Control Protocol (PPP/IPCP) address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

• Enter the name of an existing dynamic DNS method.

Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet Properties

This window enables you to configure properties for an Ethernet WAN link.

Enable PPPoE Encapsulation

Click **Enable PPPoE encapsulation** if your service provider requires that you use it. PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.

IP Address

Static IP Address

Available with PPPoE encapsulation and with no encapsulation. If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

Available with PPPoE encapsulation and with no encapsulation. If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.

IP Unnumbered

Available with PPPoE encapsulation. Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Available with PPPoE encapsulation. Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address using PPP/IPCP address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet with No Encapsulation

Use this window to configure an Ethernet connection with no encapsulation.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.

Hostname

If your service provider inserts a hostname for the router into the DHCP response that contains the dynamic IP address, you can enter that name in this field for informational purposes.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: ADSL

This window enables you to specify or edit properties of a PPPoE link supported by an ADSL connection.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.
- PPPoA specifies Point-to-Point Protocol over ATM encapsulation.
- RFC 1483 Routing (AAL5 SNAP) specifies that each PVC can carry multiple protocols.
- RFC 1483 Routing (AAL5 MUX) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation Autodetect.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Enter the VPI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Enter the VCI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.

- Unnumbered IP address—Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.

- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Hostname

If your service provider has provided a hostname for DHCP option 12, enter it here.

Operating Mode

Choose one of the following values:

- **auto**—Configure the Asymmetric Digital Subscriber Line (ADSL) after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.

- a**nsi-dmt**—Configure the ADSL line to train in the ANSI T1.413 Issue 2 mode.

- **itu-dmt**—Configure the ADSL line to train in the ITU G.992.1 mode.

- **adls2**—Configure the ADSL line to train in the ITU G.992.3 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.

- **adsl2+**—Configure the ADSL line to train in the ITU G.992.4 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.

- **splitterless**—Configure the ADSL line to train in the G.Lite mode. This mode is available for older ADSL network modules such as the WIC-1ADSL.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

✎

Note   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: ADSL over ISDN

Add or edit an ADSL over ISDN connection in this window.

Encapsulation

Choose the type of encapsulation to use for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.

- Unnumbered IP address—Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.

- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Operating Mode

Choose the mode that the ADSL line should use when training.

> **Note** If the Cisco IOS release you are running on the router does not support all five operating modes, you will see options only for the operating modes supported by your Cisco IOS release.

- **annexb**—Standard Annex-B mode of ITU-T G.992.1.

- **annexb-ur2**—ITU-T G.992.1 Annex-B mode.

- **auto**—Configure the Asymmetric Digital Subscriber Line (ADSL) line after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.

- **etsi**—European Telecommunications Standards Institute mode.

- **multimode**—Mode chosen by the firmware for the best operating condition on digital subscriber line (DSL). The final mode can be either ETSI mode or standard Annex-B mode depending on the current DSLAM setting.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

> **Note** This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: G.SHDSL

This window enables you to create or edit a G.SHDSL connection.

> **Note** If the connection that you are configuring uses a DSL controller, the Equipment Type and Operating Mode fields do not appear in the dialog.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.
- **PPPoA** specifies Point-to-Point Protocol over ATM encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation Autodetect.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Static IP address

If you choose **Static IP Address**, enter the address that the interface will use, and the subnet mask or the network bits. Obtain this information from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Dynamic IP address

If you choose Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a hostname for the router along with the IP address the router is to use. Check with your service provider or network administrator to determine the hostname sent.

IP Unnumbered

Choose this option if you want the interface to share an IP address with an Ethernet interface on the router. If you choose this option, you must specify from the drop-down list the Ethernet interface whose address you want to use.

IP Address for Remote Connection in Central Office

Enter the IP address of the gateway system to which this link will connect. This IP address is supplied by the service provider or network administrator. The gateway is the system that the router must connect to in order to access the Internet or your organization's WAN.

Equipment Type

Choose one of the values below:

CPE

Customer premises equipment. If the encapsulation type is PPPoE, CPE is automatically chosen and the field is disabled.

CO

Central office.

Operating Mode

Choose one of the values below:

Annex A (U.S.)

Configures the regional operating parameters for North America.

Annex B (Europe)

Configures the regional operating parameters for Europe.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

> **Note** This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

    Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Cable Modem

Use this dialog to change the default IP address of the cable modem service module.

Field Description

Table 6-1   Cable Modem

Element	Description
Change the default service module IP address	
Check box	Check Change the default service module IP address if you want to change the default IP address of this service module
IP Address	
Subnet Mask	You can enter the subnet mask in decimal format, or you can choose the number of bits to include in the subnet mask. 255.255.255.0 is an example of a subnet mask in decimal format. That subnet mask value is equivalent to 24 bits. Use the up arrow and the down arrow if you want to choose the number of bits. If you enter a decimal value, the bit value is automatically updated. If you enter a bit value, the decimal value is automatically updated.

Configure DSL Controller

Cisco SDM supports the configuration of the Cisco WIC-1SHDSL-V2. This WIC supports TI, E1, or a G.SHDSL connection over an ATM interface. Cisco SDM only supports a G.SHDSL connection using the ATM interface. This window lets you set the controller mode on the WIC to ATM, enabling a G.SHDSL connection, and lets you create or edit DSL controller information for the G.SHDSL connection.

Controller Mode

Cisco SDM supports only ATM mode, which provides for a G.SHDSL connection, on this controller. This field will automatically be set to ATM mode when the OK button is clicked.

Equipment Type

Choose whether your connection terminates at the central office (CO) or your customer premises equipment (CPE).

Operating Mode

Choose whether the DSL connection should use Annex A signaling (for DSL connections in the United States) or Annex B signaling (for DSL connections in Europe).

Line Mode

Choose whether this is a 2-wire or 4-wire G.SHDSL connection.

Line Number

Choose the interface number on which the connection will be made.

Line Rate

Choose the DSL line rate for the G.SHDSL port. If you have chosen a 2-wire connection, you can choose either **auto**, which configures the interface to automatically negotiate the line rate between the G.SHDSL port and the DSLAM, or the actual DSL line rate. The supported line rates are 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056, and 2312.

If you have chosen a 4-wire connection, you must choose a fixed line rate. The supported line rates for a 4-wire connection are 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608

Note   If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.

Enable Sound to Noise Ratio Margin

The sound-to-noise ratio margin provides a threshold for the DSL modem to determine whether it should reduce or increase its power output depending on the amount of noise on the connection. If you have set the line rate to "auto", you can enable this feature to maximize the quality of the DSL connection. Note that you cannot use this feature if your line rate is fixed. To enable the sound-to-noise ratio margin, check this check box and choose the ratio margins in the Current and Snext fields. To disable this feature, uncheck this check box.

Current

Choose the sound-to-noise ratio margin in the form of decibels (dB) on the current connection. The lower the ratio chosen here, the more noise will be tolerated on the connection. A lower dB setting will cause the DSL modem to allow more noise on the line, potentially resulting in a connection of lower quality but higher throughput. A higher dB setting causes the modem to restrict noise, potentially resulting in a connection of higher quality but lower throughput.

Snext

Choose the Self near-end crosstalk (Snext) sound-to-noise ratio margin in the form of decibels.

DSL Connections

This field displays all of the G.SHDSL connections currently configured on this controller. To configure a new G.SHDSL connection, click **Add**. This displays the Add a G.SHDSL Connection page, letting you configure the new connection. To edit an existing G.SHDSL connection, choose the connection in this field and click **Edit**. This also will display the Add a G.SHDSL Connection page, letting you edit the connection configuration. To delete a connection, choose the connection in this field, and click **Delete**.

Add a G.SHDSL Connection

This window enables you to create or edit a G.SHDSL connection.

Encapsulation

Select the type of encapsulation that will be used for this link.

- **PPPoE** specifies Point-to-Point Protocol over Ethernet encapsulation.

- **PPPoA** specifies Point-to-Point Protocol over ATM encapsulation.

- **RFC 1483 Routing** (**AAL5 SNAP**) specifies that each PVC can carry multiple protocols.

- **RFC 1483 Routing** (**AAL5 MUX**) specifies that each PVC carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection, and recreate it, using the encapsulation type you need.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.

IP Address

Select how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Static IP address

If you select Static IP address, enter the address that the interface will use, and the subnet mask, or the network bits. Obtain this information from your service provider or network administrator. For more information, refer to IP Addresses and Subnet Masks.

Dynamic IP address

If you select Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a host name for the router along with the IP address it is to use. Check with your service provider or network administrator to determine the host name sent.

IP Unnumbered

Select this option if you want the interface to share an IP address with an Ethernet interface on the router. If you select this option, you must specify from the drop down list the Ethernet interface whose address you want to use.

Description

Enter a description of this connection that makes it easy to recognize and manage.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to automatically update your DNS servers whenever the WAN interface's IP address changes.

> **Note** This feature appears only if supported by your Cisco server's IOS.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in Configure > Additional Tasks > Dynamic DNS Methods.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose to use an existing method. A window with a list of existing dynamic DNS methods will open. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, Frame Relay Encapsulation

Complete these fields if you are configuring a serial subinterface for Frame Relay encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

Frame Relay chosen.

IP Address

Choose either **Static IP address** or **IP unnumbered**.

IP Address

If you chose **Static IP address**, enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

If you chose **Static IP address**, enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the subnet bits. Your network administrator or service provider provides the value of the subnet mask or the network bits.

Subnet Bits

Alternatively, enter the network bits to specify how much of the IP address provides the network address.

IP Unnumbered

If you chose IP unnumbered, the interface will share an IP address that has already been assigned to another interface. Choose the interface whose IP address this interface is to share.

DLCI

Enter the data link connection identifier (DLCI) in this field. This number must be unique among all DLCIs used on this interface. The DLCI provides a unique Frame Relay identifier for this connection.

If you are editing an existing connection, the DLCI field will be disabled. If you need to change the DLCI, delete the connection and create it again.

LMI Type

Ask your service provider which of the following Local Management Interface (LMI) types you should use. The LMI type specifies the protocol used to monitor the connection:

ANSI

Annex D defined by American National Standards Institute (ANSI) standard T1.617.

Cisco

LMI type defined jointly by Cisco and three other companies.

ITU-T Q.933

ITU-T Q.933 Annex A.

Autosense

Default. This setting allows the router to detect which LMI type is used by the switch and then use that type. If autosense fails, the router will use the Cisco LMI type.

Use IETF Frame Relay Encapsulation

Check this check box to use Internet Engineering Task Force (IETF) encapsulation. This option is used to connect with routers not from Cisco. Check this box if you are connecting to a router not from Cisco on this interface.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

> **Note**   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, PPP Encapsulation

Complete these fields if you are configuring a serial interface for Point-to-Point Protocol encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

PPP chosen.

IP Address

Choose **Static IP Address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **IP Negotiated**, the router obtains an IP address from the service provider for this interface. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

> **Note** This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

    Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

    Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

    Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, HDLC Encapsulation

Fill out these fields if you are configuring a serial interface for HDLC encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

HDLC chosen.

IP Address

Choose either **Static IP address** or **IP Unnumbered**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **Static IP Address**, complete the fields below.

IP Address

Enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, choose the number of bits that specify how much of the IP address provides the network address.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

✎

Note   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

    Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

    Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

    Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Add or Edit GRE Tunnel

You can add a GRE tunnel to an interface or edit an existing interface in this window. This window does not appear if the GRE tunnel is not configured using **gre ip** mode.

Tunnel Number

Enter a number for this tunnel.

Tunnel Source

Choose the interface that the tunnel will use. This interface must be reachable from the other end of the tunnel; therefore, it must have a public, routable IP address.

Tunnel Destination

The tunnel destination is the interface on the router at the other end of the tunnel. Choose whether you will specify an IP address or a hostname, and then enter that information. If you chose IP address, provide the IP address and subnet mask in dotted decimal format; for example, 192.168.20.1 and 255.255.255.0.

Make sure that this address or hostname is reachable using the **ping** command; otherwise, the tunnel will not be properly created.

Tunnel IP Address

Enter the IP address of the tunnel in dotted decimal format; for example, 192.168.20.1. For more information, see IP Addresses and Subnet Masks.

GRE Keepalive Check Box

Check if you want the router to send GRE keepalives. Specify the interval, in seconds, that keepalives will be sent, and the waiting period, in seconds, between retries.

Maximum Transmission Unit

Enter the maximum transmission unit (MTU) size. If you want the size adjusted to a lower value when the adjustment would avoid packet fragmentation, click **Adjust MTU to avoid fragmentation**.

Bandwidth

Click to specify the bandwidth for this tunnel in kilobytes.

Connection: ISDN BRI

Complete these fields if you are configuring an ISDN BRI connection. Because Cisco SDM supports only PPP encapsulation over an ISDN BRI connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

ISDN Switch Type

Choose the ISDN switch type. Contact your ISDN service provider for the switch type for your connection.

Cisco SDM supports these BRI switch types:

- For North America:
    - basic-5ess—Lucent (AT&T) basic rate 5ESS switch
    - basic-dms100—Northern Telecom DMS-100 basic rate switch
    - basic-ni—National ISDN switches
- For Australia, Europe, and the UK:
    - basic-1tr6—German 1TR6 ISDN switch
    - basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
    - vn3—French ISDN BRI switches
- For Japan:
    - ntt—Japanese NTT ISDN switches
- For Voice/PBX systems:
    - basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931 ()

SPIDs

Click if you need to enter service profile ID (SPID) information.

Some service providers use SPIDs to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The Lucent (AT&T) 5ESS switch type may support a SPID, but we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

Remote Phone Number

Enter the phone number of the destination of the ISDN connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic, enter timer settings, or enable or disable multilink PPP.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Multilink PPP can be configured to provide load balancing between ISDN B channels.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Analog Modem

Complete these fields if you are configuring an analog modem connection. Because Cisco SDM supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

> **Note**   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

    Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

    Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

    Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: (AUX Backup)

Complete these fields if you are configuring an asynchronous dial-up connection using the console port to double as an AUX port on a Cisco 831 or 837 router. Once you enter the information in this window, click **Backup Details** and enter dial-backup information, which is required for this type of connection. Note that because Cisco SDM supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

The option to configure the AUX port as a dial-up connection appears only for the Cisco 831 and 837 routers. This option will not be available for those routers if any of the following conditions occur:

- Router is not using a Zutswang Cisco IOS release
- Primary WAN interface is not configured
- Asynchronous interface is already configured
- Asynchronous interface is not configurable by Cisco SDM because of the presence of unsupported Cisco IOS commands in the existing configuration

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Backup Details

Click to display the Backup Configuration window, which lets you configure dial-backup information for this connection. This information is mandatory for this type of connection, and an error will be displayed if you try to complete the connection configuration without entering dial-backup configuration information.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note   This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Additional Tasks > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Authentication

This page is displayed if you enabled PPP for a serial connection or PPPoE encapsulation for an ATM or Ethernet connection, or you are configuring an ISDN BRI or analog modem connection. Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

CHAP/PAP

Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes: the router will attempt both types of authentication, and one attempt will succeed.

CHAP authentication is more secure than PAP authentication.

Login Name

The login name is given to you by your service provider and is used as the username for CHAP/PAP authentication.

Password

Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password *test* is not the same as *TEST*.

Reenter Password

Reenter the same password that you entered in the previous box.

SPID Details

Some service providers use service profile ID numbers (SPIDs) to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, and we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

SPID1

Enter the SPID to the first BRI B channel provided to you by your ISP.

SPID2

Enter the SPID to the second BRI B channel provided to you by your ISP.

Dialer Options

Both ISDN BRI and analog modem interfaces can be configured for dial-on-demand routing (DDR), which causes the connection to dial out and become active only under specified circumstances, thus saving connection time and cost. This window lets you configure options specifying when ISDN BRI or analog modem connections should be initiated and ended.

Dialer List Association

The dialer list lets you associate the ISDN BRI or analog modem connection with an ACL to identify *interesting traffic*. Identifying interesting traffic will cause the interface to dial out and establish a connection only when the router detects data traffic that matches the ACL.

Allow all IP traffic

Choose this option to cause the interface to dial out and establish a connection whenever there is any IP traffic being sent over the interface.

Filter traffic based on selected ACL

Choose this option to associate an ACL, which must be created using the rules interface, with the interface. Only traffic that matches the traffic identified in the ACL will cause the interface to dial out and establish a connection.

You can enter the ACL number you want to associate with the dialer interface to identify interesting traffic, or you can click the button next to the field to browse the list of ACLs or create a new ACL and choose it.

Timer Settings

Timer settings let you configure the maximum amount of time that a connection with no traffic stays active. By configuring timer settings, you can have connections that shut down automatically, saving you connection time and cost.

Idle timeout

Enter the number of seconds that are allowed to pass before an idle connection (one that has no traffic passing over it) is terminated.

Fast idle timeout

The fast idle timeout is used when one connection is active while a competing connection is waiting to be made. The fast idle timeout sets the maximum number of seconds with no interesting traffic before the active connection is terminated and the competing connection is made.

This occurs when the interface has an active connection to a next hop IP address and the interface receives interesting data with a different next hop IP destination. Because the dialer connection is point-to-point, the competing packet cannot be delivered until the current connection is ended. This timer sets the amount of time that must pass while the first connection is idle before that connection will be terminated and the competing connection made.

Enable Multilink PPP

Multilink PPP lets you load-balance data over multiple ISDN BRI B channels and asynchronous interfaces. With multilink PPP, when an ISDN connection is initially made, only one B channel is used for the connection. If the traffic load on the connection exceeds the specified threshold (entered as a percentage of total bandwidth), then a connection with a second B channel is made, and the data traffic is shared over both connections. This has the advantage of reducing connection time and cost when data traffic is low, and letting you use your full ISDN BRI bandwidth when it is needed.

Check this check box if you want to enable multilink PPP. Uncheck it if you do not.

Load Threshold

Use this field to configure the percentage of bandwidth that must be used on a single ISDN BRI channel before another ISDN BRI channel connection will be made to load-balance traffic. Enter a number between 1 and 255, where 255 equals 100 percent of bandwidth on the first connection being utilized.

Data Direction

Cisco SDM supports Multilink PPP only for outbound network traffic.

Backup Configuration

ISDN BRI and analog modem interfaces can be configured to work as backup interfaces to other, primary interfaces. In that case, an ISDN or analog modem connection will be made only if the primary interface goes down for some reason. If the primary interface and connection go down, the ISDN or analog modem interface will immediately dial out and try to establish a connection so that network services are not lost.

Enable Backup

Check if you want this ISDN BRI or analog modem interface to act as a backup connection. Uncheck this check box if you do not want the ISDN BRI or analog modem interface to be a backup interface.

Primary Interface

Choose the interface on the router that will maintain the primary connection. The ISDN BRI or analog modem connection will only be made should the connection on the chosen interface go down.

Tracking Details

Use this section to identify a specific host to which connectivity must be maintained. The router will track connectivity to that host, and if the router discovers that connectivity to the host specified was lost by the primary interface, this will initiate a backup connection over the ISDN BRI or analog modem interface.

Hostname or IP Address to be Tracked

Enter the hostname or IP address of the destination host to which connectivity will be tracked. Specify an infrequently contacted destination as the site to be tracked.

Track Object Number

This is a read-only field that displays an internal object number generated and used by Cisco SDM for tracking the connectivity to the remote host.

Next Hop Forwarding

These fields are optional. You can enter the IP address to which the primary and backup interfaces will connect when they are active. This is known as the next hop IP address. If you do not enter next hop IP addresses, Cisco SDM will configure static routes using the interface name. Note that when you back up a multipoint WAN connection, such as an Ethernet connection, you must enter next hop IP addresses in order for routing to occur properly, but when backing up a point-to-point connection, this information is not necessary.

Primary Next Hop IP Address

Enter the next hop IP address of the primary interface.

Backup Next Hop IP Address

Enter the next hop IP address of the ISDN BRI or analog modem backup interface.

Delete Connection

You can delete a WAN connection that appears in the Edit Interface/Connections window. This window appears when you are deleting an interface configuration, and when the connection you want to delete contains associations such as access rules that have been applied to this interface. This window gives you the opportunity to save the associations for use with another connection.

When you delete a connection, the Create New Connection list is refreshed if the deletion makes a connection type available that was not available before the deletion.

You can automatically delete all associations that the connection has, or delete the associations later.

To view the associations that the connection has:

Click **View Details**.

To delete the connection and all associations:

Click **Automatically delete all associations**, and then click **OK** to cause Cisco SDM to delete the connection and all of the associations.

To manually delete the associations:

To manually delete the associations, click **View Details** to see a list of the associations that this connection has. Make note of the associations, choose **I will delete the associations later**, and then click **OK**. You can manually delete the associations using the instructions in the following list.

The possible associations and the instructions for deleting them are:

- Default Static Route—The interface is configured as the forwarding interface for a default static route. To delete the static route with which this interface is associated, click **Configure**, then click **Routing**. Click the static route in the Static Routing table, and click **Delete**.

- Port Address Translation—PAT is configured, using the interface on which this connection was created. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and click **Delete**.

- NAT—The interface is designated as either a NAT inside or NAT outside interface. To delete the NAT association, click **Configure**, then click **Interfaces and Connections**. Click the connection in the interface list, and then click **Edit**. Click the **NAT** tab, then choose **None** from the NAT drop-down menu.

- ACL—An ACL is applied to the interface on which the connection was created. To delete the ACL, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association tab**, then in the Access Rule group, click the **...** button next to both the Inbound and Outbound fields, and click **None**.

- Inspect—An inspection rule is applied to the interface on which the connection was created. To delete the inspection rule, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association tab**, then in the Inspection Rule group, for both the Inbound and Outbound fields, choose **None**.

- Crypto—A crypto map is applied to the interface on which the connection was created. To delete the crypto map, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, then in the VPN group, in the IPSec Policy field, click **None**.

- EZVPN—An Easy VPN is applied to the interface on which the connection was created. To delete the Easy VPN, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, then in the VPN group, in the Easy VPN field, click **None**.

- VPDN—VPDN commands that are required for a PPPoE configuration are present in the router configuration. If there are any other PPPoE connections configured on the router, do not delete the VPDN commands.

- ip tcp adjust mss—This command is applied to a LAN interface to adjust the TCP maximum size. If there are any other PPPoE connections configured on the router, do not delete this command.

- Backup connection—When a backup connection is configured for the primary interface.To delete the backup association, click **Configure**, then click **Interfaces and Connections**. Click the Backup interface in the Interface List, then click **Edit**. Click the **Backup** tab and uncheck the **Enable Backup** check box.

- PAT on Backup connection—PAT is configured on the backup interface. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and then click **Delete**.

- Floating Default Route on Backup connection—The Backup interface is configured with a floating default static route. To delete the floating static route, click **Configure**, then click **Routing**. Click the floating static route in the Static Routing table, and click **Delete**.

Connectivity Testing and Troubleshooting

This window allows you to test a configured connection by pinging a remote host. If the ping fails, Cisco SDM reports the probable cause and suggests actions you can take to correct the problem.

Which connection types can be tested?

Cisco SDM can troubleshoot ADSL, G.SHDSL V1 and G.SHDSL V2 connections, using PPPoE, AAL5SNAP or AAL5MUX encapsulation.

Cisco SDM can troubleshoot Ethernet connections with PPPoE encapsulation.

Cisco SDM cannot troubleshoot unencapsulated Ethernet connections, Serial and T1 or E1 connections, Analog connections, and ISDN connections. Cisco SDM provides basic ping testing for these connection types.

What is Basic Ping Testing?

When Cisco SDM performs basic ping testing, it does the following:

1. Checks the interface status to see if it is up or down.

2. Checks DNS Settings, whether they be Cisco SDM default options or user-specified hostnames.

3. Checks for DHCP and IPCP configurations on the interface.

4. Exits interface test.

5. Pings the destination.

Cisco SDM reports the results of each of these checks in the Activity/Status columns. If the ping succeeds, then the connection will be reported as successful. Otherwise the connection is reported down, and the test that failed is noted.

How does Cisco SDM Troubleshoot?

When Cisco SDM troubleshoots a connection, it performs a more extensive check than the basic ping test. If the router fails a test, Cisco SDM performs additional checks so it can provide you with the possible reasons for failure. For example, if Layer 2 status is down, Cisco SDM attempts to determine the reason(s), reports them, and recommends actions you can take to rectify the problem. Cisco SDM performs the following tasks:

1. Checks interface status. If the Layer 2 protocol is up, Cisco SDM goes to step 2.

   If Layer 2 protocol status is down, Cisco SDM checks ATM PVC status for XDSL connections, or PPPoE status for encapsulated Ethernet connections.

   – If the ATM PVC test fails, Cisco SDM displays possible reasons for the failure and actions you can take to correct the problem.

   – If the PPPoE connection is down, there is a cabling problem, and Cisco SDM displays appropriate reasons and actions.

   After performing these checks, the test is terminated and Cisco SDM reports the results and suggests actions.

2. Checks DNS Settings, whether they be Cisco SDM default options or user-specified hostnames.

3. Checks DHCP or IPCP configuration and status. If the router has an IP address through either DHCP or IPCP Cisco SDM goes to step 4.

   If the router is configured for DHCP or IPCP but has not received an IP address through either of these methods, Cisco SDM performs the checks in step 1. The test terminates and Cisco SDM reports the results and suggests actions.

4. Pings the destination. If the ping succeeds, Cisco SDM reports success.

If the ping fails on an xDSL connection with PPPoE encapsulation, Cisco SDM checks:

- the ATM PVC status

- the PPPoE tunnel status

- the PPP authentication status

After performing these checks, Cisco SDM reports the reason that the ping failed.

If the ping fails on an Ethernet with PPPoE encapsulation connection, Cisco SDM checks:

- the PPPoE tunnel status

- the PPP authentication status

After performing these checks, Cisco SDM reports the reason that the ping failed.

If the ping fails on an xDSL connection with AAL5SNAP or AAL5MUX encapsulation, Cisco SDM checks the ATM PVC status and reports the reason the ping failed.

IP Address/Hostname

Specify the server name to ping to test WAN interface.

Automatically determined by SDM

Cisco SDM pings its default host to test WAN interface. Cisco SDM detects the router's statically configured DNS servers, and dynamically imported DNS servers. Cisco SDM pings these servers, and if successful pings exit through the interface under test, Cisco SDM reports success. If no pings succeeded, or successful pings were not found to exit the interface under test, Cisco SDM reports failure.

User Specified

Specify the IP address of hostname of your choice for testing WAN interface.

Summary

Click this button if you want to view the summarized troubleshooting information.

Details

Click this button if you want to view the detailed troubleshooting information.

Activity

This column displays the troubleshooting activities.

Status

Displays the status of each troubleshooting activity by the following icons and text alerts:

    The connection is up.

    The connection is down.

    Test is successful.

    Test failed.

Reason

This box provides the possible reason(s) for the WAN interface connection failure.

Recommended action(s)

This box provides a possible action/solution to rectify the problem.

What Do You Want to Do?

If you want to:	Do this:
Troubleshoot the WAN interface connection.	Click **Start** button. When test is running, **Start** button label will change to **Stop**. You have option to abort the troubleshooting while test is in progress.
Save the test report.	Click **Save Report** button to save the test report in HTML format. This button will be active only when test is in progress or when the testing is complete.

C H A P T E R 7

Wide Area Application Services

Cisco's Wide Area Application Services (WAAS) is a WAN optimization and application acceleration solution that enables branch office server consolidation, improves performance for centralized applications, and provides remote users with LAN-like access to applications, storage, and content across the WAN.

The WAAS solution has three major components:

- Wide Area Engine Edge—(WAE-E). The edge WAE is installed on clients. It is a file caching device that serves client requests at remote sites and branch offices. The device is deployed at each branch office or remote campus, replacing file servers and print servers, giving local clients fast, near-LAN read and write access to a cached view of data residing at a remote data center.

- Wide Area Engine Core—(WAE-C). The core WAE component is installed on a server at the data center. It connects directly to one or more file servers or network-attached storage (NAS) devices. Core WAEs are placed between the file servers at the data center and the WAN that connects the data center to the enterprise's remote sites and branch offices. Requests that are received from edge WAEs are translated by the core WAE into the original file server protocol and forwarded to the appropriate file server. The core WAEs at the data center can provide load balancing and failover support.

- Web Cache Communication Protocol—(WCCP). This is a Cisco protocol that specifies interactions between one or more routers or Layer 3 switches, and one or more application appliances, web caches, and caches of other protocols. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers to a group of appliances. Any type of TCP traffic can be redirected.

This chapter contains the help topics for the WAAS configuration screens and contains the following sections:

- Configuring a WAAS Connection
- WAAS Reference

Configuring a WAAS Connection

You must have a WAAS network interface module installed on the router in order to configure WAAS.

Complete the following steps to configure a WAAS connection:

Step 1   If you want to review the Cisco IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit** > **Preferences** > **Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM toolbar, click **Interfaces** and **Connections**.

Step 4   Click the **NM WAAS** tab, next to the Edit Interface/Connection tab.

Step 5   Click **Edit Settings** to configure the router for the WAAS network module.

    a.   Enter the required information in the Integrated Services Engine tab. See Integrated Service Engine for more information

    b.   Click **WCCP**, and enter the required information in the WCCP tab. See WCCP for more information.

Step 6   Click **OK** to return to the NM WAAS tab.

Step 7   If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it. If you did not make this setting, clicking OK sends the configuration to the router.

Step 8   In the Tools menu, click **Telnet**.

Step 9   Enter the router username and password.

Step 10 If necessary, enter the **enable** command, press **Enter**, and provide the enable password.

Step 11 At the Cisco IOS command prompt, enter the following commands:

```
Router(config)# wccp router-list 1 default_gateway
Router(config)# wccp tcp-promiscuous router-list-num 1
Router(config)# wccp version 2
```

Replace *default_gateway* with the IP address of the router that provides a route to the CM.

Step 12 In the NM WAAS tab, click **Register**.

   a. Enter the IP address of the WAAS CM.

   b. Choose the interface on which you want to send the registration request. The interface that you choose must have a route to the WAAS CM network.

   c. Click **OK**. Cisco SDM displays a username and password dialog box.

   d. Enter the username and password required to login to the CM.

After the router registers with the CM, the blue https link contains the CM IP address.

Step 13 Click on the https link to view the registration status for the Edge WAE on the router. The CM displays the device registration status as online.

WAAS Reference

The following sections describe the WAAS configuration screens:

- NM WAAS
- Integrated Service Engine
- WCCP
- Central Manager Registration

NM WAAS

If a WAAS network module is installed on the router, Cisco SDM shows the NM WAAS tab. This tab shows the current WAAS status and configuration, and from this tab you can go to the WAAS configuration screens.

From this screen, Cisco SDM allows you to log in to the WAAS Central Manager (CM) so that you can register the edge WAE, and view the registration status sent by the CM.

> **Note**   Do not click the Register button at the top of the screen until you configure the WAAS NM and enter these Cisco IOS global configuration mode CLI commands:
>
> ```
> Router(config)# wccp router-list 1 default_gateway
> Router(config)# wccp tcp-promiscuous router-list-num 1
> Router(config)# wccp version 2
> ```
>
> Replace *default_gateway* with the IP address of the router that provides a route to the CM. See Configuring a WAAS Connection for more information.

Related Links

- Configuring a WAAS Connection

Field Reference

Table 7-1 describes the information in the NM WAAS tab.

Table 7-1   *NM WAAS Tab*

Element	Description
Registration status with the WAAS central manager	Cisco SDM shows one of the following: • Active—The Edge WAE is registered with the WAAS central manager. Cisco SDM displays a green icon when the Edge WAE is registered. • Inactive—The Edge WAE is not registered with the WAAS central manager. Cisco SDM displays a red icon when the Edge WAE is not registered.
Register	To log on to the CM and register the Edge WAE on the router, click **Register**. ✎ **Note** Do not attempt to register until you have configured the WAAS NM, and entered the Cisco IOS CLI commands noted at the beginning of this help topic.
Refresh	To refresh the registration status, click **Refresh**. Cisco SDM displays a username and password dialog to allow you to login to the CM.
To configure the WAAS device....	To launch the central manager device manager, click on the displayed link.
WAAS Configuration	
WAAS Interface	The name of the WAAS network module; for example, Integrated Service Engine 0/0.
Router IP address	The IP address of the router interface to the service module. This is the IP address of the Redirect interface.
Service Module Internal IP Address	The internal IP address assigned to the service module.
Service Module External IP Address	(Optional). The external IP address assigned to the service module.
Default Gateway	The default gateway IP address used by the service module.
WCCP Protocol Settings	

Table 7-1   NM WAAS Tab (continued)

Element	Description
Version	The version of the WCCP protocol in use; for example, WCCP Version 2.
Inside Interface	The name of the router interface being used for the WCCP inside interface. This interface is connected to the LAN.
Outside Interface	The name of the router interface being used for the WCCP outside interface. This interface is connected to the WAN.
Redirect Interface	The router interface that is redirecting traffic to the WAAS service module. This interface is configured to avoid redirection loops.
Buttons	
Edit Settings	Click **Edit Settings** to display a dialog that enables you to change integrated service engine settings and WCCP settings.
Delete	Click **Delete** to remove the current WAAS configuration.
Reload	Click **Reload** to refresh the information in this screen.

Integrated Service Engine

Enter settings for the router, the WAAS service module, and the gateway that the service module uses in this screen.

Field Reference

Table 7-2 describes the configuration fields in this screen.

Table 7-2   Integrated Service Engine Tab

Element	Description
Router IP Address	
IP Address	Enter the IP address of the router interface that is to redirect traffic to the WAAS service module.

Table 7-2   Integrated Service Engine Tab (continued)

Element	Description
Subnet mask	Enter the subnet mask in decimal format; for example, 255.255.255.0. Or, choose the number of subnet bits; for example, 24. Entering values in one field updates the other. For example, if you enter 255.255.255.0, the subnet bits field is automatically updated to display 24.
Service Module	
Internal IP Address	Enter the internal IP address of the WAAS network module. This IP address must be on the same subnet as the router IP address used. For example, if the router IP address is 10.0.0.20, the service module internal IP address might be 10.0.0.21.
Subnet Mask	Enter the subnet mask in decimal format; for example, 255.255.255.0. Or, choose the number of subnet bits; for example, 24. Entering values in one field updates the other. For example, if you enter 255.255.255.0, the subnet bits field is automatically updated to display 24.
External IP Address	(Optional). Enter the external IP address for the WAAS network module. This IP address may be required to connect to the WAAS CM.
Subnet Mask	Enter the subnet mask in decimal format; for example, 255.255.255.0. Or, choose the number of subnet bits; for example, 24. Entering values in one field updates the other. For example, if you enter 255.255.255.0, the subnet bits field is automatically updated to display 24.
Default Gateway	
Default Gateway IP Address	Enter the IP address of the default gateway router that the WAAS service module is to use.

WCCP

Configure WCCP settings in this screen. WCCP settings specify the router interfaces that redirect traffic to the WAAS NM, and information about the WAAS CM.

Field Reference

Table 7-3 describes the fields in this screen.

Table 7-3   WCCP Tab Field Reference

Element	Description
WCCP Settings	
WCCP 61 Redirect	Choose the LAN subinterface from the list that carries the traffic that you want to redirect to the WAAS NM. The interface that you choose is displayed as the Inside Interface on the NM WAAS tab. Choose IN from the list to the right of the interface list.
WCCP 62 Redirect	Choose the WAN subinterface from the list that carries the traffic that you want to redirect to the WAAS NM. he interface that you choose is displayed as the Outside Interface on the NM WAAS tab. Choose IN from the list to the right of the interface list.
WCCP Redirect Exclude	Choose the Integrated Services Engine used in this configuration to specify that the router is not to repeatedly redirect the same traffic to the local WAE.

Central Manager Registration

In this screen, register with the WAAS Central Manager.

Field Reference

Table 7-4 describes the fields in this screen

Table 7-4   WAAS Central Manager Registration

Element	Description
IP Address	Enter the IP Address of the WAAS Central Manager.
Primary Interface	Choose the router interface on which the registration request should be sent. The interface must have a route to the WAAS Central Manager's network.

C H A P T E R 8

Create Firewall

A firewall is a set of rules used to protect the resources of your LAN. These rules filter the packets arriving at the router. If a packet does not meet the criteria specified in the rule, it is dropped. If it does meet the criteria, it is allowed to pass through the interface that the rule is applied to. This wizard enables you to create a firewall for your LAN by answering prompts in a set of screens.

In this window, select the type of firewall that you want to create.

Note
- The router that you are configuring must be using a Cisco IOS image that supports the Firewall feature set in order for you to be able to use Cisco Router and Security Device Manager (Cisco SDM) to configure a firewall on the router.
- The LAN and WAN configurations must be complete before you can configure a firewall.

Basic Firewall

Click this if you want Cisco SDM to create a firewall using default rules. The use case scenario shows a typical network configuration in which this kind of firewall is used.

Advanced Firewall

Click this if you want Cisco SDM to lead you through the steps of configuring a firewall. You have the option to create a DMZ network, and to specify an inspection rule. The use case scenario shown when you select this option shows you a typical configuration for an Internet of firewall.

What Do You Want to Do?

If you want to:	Do this:
Have Cisco SDM create a firewall for me. You might want to select this option if you do not want to configure a DMZ network, or if there is only one outside interface.	Click **Basic Firewall**. Then, click **Launch the Selected Task**. Cisco SDM asks you to identify the interfaces on your router, and then it uses Cisco SDM default access rules and inspection rules to create the firewall.

If you want to:	Do this:
Have Cisco SDM help me create an Advanced Firewall. If your router has multiple inside and outside interfaces, and you want to configure a DMZ, you should select this option.	Select **Advanced Firewall**. Then, click **Launch the Selected Task**. Cisco SDM will show you the default inspection rule and allow you to use it in the firewall. Or, you can create your own inspection rule. Cisco SDM will use a default access rule in the firewall
Get information about a task that this wizard does not help me complete.	Select a topic from the following list: • How Do I View Activity on My Firewall? • How Do I Configure a Firewall on an Unsupported Interface? • How Do I Configure a Firewall After I Have Configured a VPN? • How Do I Permit Specific Traffic Through a DMZ Interface? • How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host? • How Do I Configure NAT on an Unsupported Interface? • How Do I Configure NAT Passthrough for a Firewall? • How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator? • How Do I Associate a Rule with an Interface? • How Do I Disassociate an Access Rule from an Interface • How Do I Delete a Rule That Is Associated with an Interface? • How Do I Create an Access Rule for a Java List? • How Do I View the IOS Commands I Am Sending to the Router? • How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?

Basic Firewall Configuration Wizard

Cisco SDM will protect the LAN with a default firewall when you select this option. For Cisco SDM to do this, you must specify the inside and outside interfaces in the next window. Click **Next** to begin configuration.

Basic Firewall Interface Configuration

Identify the interfaces on the router so that the firewall will be applied to the correct interface.

Outside (untrusted) Interface

Select the router interface that is connected to the Internet or to your organization's WAN.

Note Do not select the interface through which you accessed Cisco SDM as the outside (untrusted) interface. Doing so will cause you to lose your connection to Cisco SDM. Because it will be protected by a firewall, you will not be able to launch Cisco SDM from the outside (untrusted) interface after the Firewall Wizard completes.

Allow secure Cisco SDM access from outside interfaces checkbox

Check this box if you want users outside the firewall to be able to access the router using Cisco SDM. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If youspecify a network address, all hosts on that network willbe allowed through the firewall.

Inside (trusted) Interfaces

Check the physical and logical interfaces connecting to the LAN. You can select multiple interfaces.

Configuring Firewall for Remote Access

Creating a firewall can block access to the router that remote administrators may need. You can specify the router interfaces to use for remote management access and the hosts from which administrators can log on to Cisco SDM to manage the router. The firewall will be modified to allow secure remote access from the host or network that you specify.

Select the outside interface

If you are using the Advanced Firewall wizard, select the interface through which users are to launch Cisco SDM. This field does not appear in the Basic Firewall wizard.

Source Host/Network

If you want to allow a single host access through the firewall, choose **Host Address** and enter the IP address of a host. Choose **Network Address** and enter the address of a network and a subnet mask to allow hosts on that network access through the firewall. The host or network must be accessible from the interface that you specified. Choose **Any** to allow any host connected to the specified interfaces secure access to the network.

Advanced Firewall Configuration Wizard

Cisco SDM will help you create an Internet firewall by asking you for information about the interfaces on the router, whether you want to configure a DMZ network, and what rules you want to use in the firewall.

Click **Next** to begin configuration.

Advanced Firewall Interface Configuration

Identify the router's inside and outside interfaces and the interface that connects to the DMZ network.

Check **outside** or **inside** to identify each interface as an outside or an inside interface. Outside interfaces connect to your organizations's WAN or to the Internet. Inside interfaces connect to your LAN.

Allow secure Cisco SDM access from outside interfaces checkbox

Check this box if you want users outside the firewall to be able to access the router using Cisco SDM. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If youspecify a network address, all hosts on that network willbe allowed through the firewall.

DMZ Interface

Select the router interface that connects to a DMZ network, if one exists. A DMZ network is a buffer zone used to isolate traffic that comes from an untrusted network. If you have a DMZ network, select the interface that connects to it.

Advanced Firewall DMZ Service Configuration

This window allows you to view rule entries that specify which services available inside the DMZ you want to make available through the router's outside interfaces. Traffic of the specified service types will be allowed through the outside interfaces into the DMZ network.

DMZ Service Configuration

This area shows the DMZ service entries configured on the router.

Start IP Address

The first IP address in the range that specifies the hosts in the DMZ network.

End IP Address

The last IP address in the range that specifies the hosts in the DMZ network. If there is no value listed in this column, the IP address in the Start IP address column is presumed to be the only host in the DMZ network. The range can specify a maximum of 254 hosts.

Service Type

The type of service, either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Service

The name of the service, such as Telnet, or FTP, or a protocol number.

To configure a DMZ service entry:

Click **Add**, and create the entry in the DMZ Service Configuration window.

To edit a DMZ service entry:

Select the service entry, and click **Edit**. Then, edit the entry in the DMZ Service Configuration window.

DMZ Service Configuration

Create or edit a DMZ service entry in this window.

Host IP Address

Enter the address range that will specify the hosts in the DMZ that this entry applies to. The firewall will allow traffic for the specified TCP or UDP service to reach these hosts.

Start IP Address

Enter the first IP address in the range; for example, 172.20.1.1. If Network Address Translation (NAT) is enabled, you must enter the NAT-translated address, known as the *inside global* address.

End IP Address

Enter the last IP address in the range; for example, 172.20.1.254. If NAT is enabled, you must enter the NAT-translated address.

Service

TCP

Click this option if you want to allow traffic for a TCP service.

UDP

Click this option if you want to allow traffic for a UDP service.

Service

Enter the service name or number in this field. If you do not know the name or number, click the button and select the service from the list displayed.

Application Security Configuration

Cisco SDM provides preconfigured application security policies that you can use to protect the network. Use the slider bar to select the security level that you want and to view a description of the security it provides. The wizard summary screen displays the policy name, SDM_HIGH, SDM_MEDIUM, or SDM_LOW and the configuration statements in the policy. You can also view the details of the policy by clicking the Application Security tab and choosing the name of the policy.

Preview Commands Button

Click to view the IOS commands that make up this policy.

Custom Application Security Policy Button

This button and the Policy Name field are visible if you are completing the Advanced Firewall wizard. Choose this option if you want to create your own application security policy. If the policy already exists, enter the name in the field, or click the button on the right, choose **Select an existing policy**, and select the policy. To create a policy, click the button, choose **Create a New Policy**, and create the policy in the dialog displayed.

Domain Name Server Configuration

The router must be configured with the IP address of at least one DNS server for application security to work. Click **Enable DNS-based hostname**-**to-address** translation, and provide the IP address of the primary DNS server. If a secondary DNS server is available, enter it's IP address in the **Secondary DNS Server** field.

The IP addresses that you enter will be visible in the DNS Properties window under Additional Tasks.

URL Filter Server Configuration

URL filter servers are capable of storing and maintaining much more URL filtering information than a router configuration file can contain. If there are URL filter servers on the network, you can configure the router use them. You can configure additional URL filter server parameters by going to **Configure** > **Additional Tasks** > **URL Filtering**. See URL Filtering for more information.

Filter HTTP Request through URL Filter Server

Check the **Filter HTTP Request through URL Filter Server** box to enable URL filtering by URL filter servers.

URL Filter Server Type

Cisco SDM supports the Secure Computing and Websense URL filter servers. Choose either **Secure Computing** or **Websense** to specify the type of URL filter server on the network.

IP Address/Hostname

Enter the IP address or the hostname of the URL filter server.

Select Interface Zone

This window appears if a router interface other than the one you are configuring is a member of a Zone-Based Policy Firewall security zone. For more information about this topic, see Zone-Based Policy Firewall.

Select Zone

> Select the security zone that you want the interface to be a member of. If you choose not to assign the interface to a zone, there is a strong possibility that traffic will not pass through the interface.

ZPF Inside Zones

> Zones that include interfaces used in generic routing encapsulation (GRE) tunnels must be designated as inside (trusted) zones in order for GRE traffic to pass through the firewall.

> This window lists the configured zones and their member interfaces. To designate a zone as inside, check the **inside** (**trusted**) column in the row for that zone.

Voice Configuration

> Include voice traffic in the router firewall policy by providing the necessary information in this screen.

> **Field Reference**

> Table 8-1 describes the fields in this screen.

Table 8-1   *Voice Configuration Fields*

Element	Description
Enable Voice Configuration	Check **Enable Voice Configuration** to enable the other fields in this screen.
Interface	The name of a router interface, for example, GigabitEthernet0/1
Outside (untrusted)	Check **Outside** (**untrusted**) next to the interface name if you are using the interface to connect to the WAN.
Inside (trusted)	Check **Inside** (**trusted**) next to the interface name if you are using the interface to connect to the LAN or other trusted network.

Table 8-1   Voice Configuration Fields

Element	Description
Select the Lineside Protocol	The lineside protocol is the protocol used when sending traffic too and from the phones on the network. Choose one of the following options: • SIP—Session Initiation Protocol. • SCCP—Skinny Client Control Protocol.
Select the Trunkside Protocol	The trunkside protocol is the protocol used when sending traffic over the Internet. Choose one of the following options: • SIP—Session Initiation Protocol. • H.323
Enable logging for voice traffic	To view logging messages related to voice traffic in the monitor screens, check **Enable logging for voice traffic**. To view these messages, click **Monitor** in the Cisco SDM toolbar, and then click **Firewall**.

Summary

This screen summarizes the firewall information. You can review the information in this screen and use the Back button to return to screens in the wizard to make changes.

The summary screen uses plain-language to describe the configuration. You can view the CLI commands that Cisco SDM delivers to the router by going to Edit > Prefereences, and checking **Preview commands before delivering to router**.

Inside (trusted) Interface(s)

Cisco SDM lists the router's logical and physical interfaces that you designated as the inside interfaces in this wizard session, along with their IP addresses. Underneath, plain-language descriptions are given for each configuration statement applied to the inside interfaces . The following are examples:

```
Inside(trusted) Interfaces:
FastEthernet0/0 (10.28.54.205)
Apply access rule to the inbound direction to deny spoofing traffic.
```

```
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback address.
Apply access rule to the inbound direction to permit all other
traffic.
Apply application security policy SDM_HIGH to the inbound direction.
```

This example shows the Cisco SDM Application Security policy SDM_HIGH applied to inbound traffic on this interface.

Outside (untrusted) Interface(s)

Cisco SDM lists the router logical and physical interfaces that you designated as outside interfaces in this wizard session, along with their IP addresses. Underneath, plain-language descriptions are given for each configuration statement applied to the outside interfaces. The following are examples:

```
FastEthernet0/1 (142.120.12.1)
Turn on unicast reverse path forwarding check for non-tunnel
interfaces.
Apply access rule to the inbound direction to permit IPSec tunnel
traffic if necessary.
Apply access rule to the inbound direction to permit GRE tunnel
traffic for interfaces if necessary.
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if
necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback and private address.
Apply access rule to the inbound direction to permit service traffic
going to DMZ interface.
Service ftp at 10.10.10.1 to 10.10.10.20
Apply access rule to the inbound direction to permit secure SDM access
from 140.44.3.0 255.255.255.0 host/network
Apply access rule to the inbound direction to deny all other traffic.
```

Note that this configuration turns on reverse path forwarding, a feature that allows the router to discard packets that lack a verifiable source IP address, and permits ftp traffic to the DMZ addresses 10.10.10.1 through 10.10.10.20.

DMZ Interface

If you configured an Advanced firewall, this area shows you the DMZ interface you designated, along with its IP address. Underneath, Cisco SDM describes what access and inspection rules were associated with this interface. The following are examples:

```
FastEthernet (10.10.10.1)
Apply CBAC inspection rule to the outbound direction
Apply access rule to the inbound direction to deny all other traffic.
```

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the User Preferences window, the Deliver configuration to router window appears. In this window, you can view the CLI commands you that are delivering to the router.

SDM Warning: SDM Access

This window appears when you have indicated that Cisco SDM should be able to access the router from outside interfaces. It informs you that you must ensure that SSH and HTTPS are configured, and that at least one of the interfaces designated as outside be configured with a static IP address. To do this, you must ensure that an outside interface is configured with a static IP address, and then associate a management policy with that interface.

Determining if an Outside Interface is Configured with a Static IP Address

Complete the following steps to determine if an outside interface is configured with a static IP address.

Step 1   Click **Configure > Interfaces and Connections > Edit Interface/Connection**.

Step 2   Review the IP column in the Interface list table to determine if an outside interface has a static IP addresses.

Step 3   If no outside interface has a static IP address, select one and click **Edit** to display a dialog that allows you to reconfigure the IP address information for the interface.

If there is anoutside interface with a static IP address, note that interface name and complete the next procedure.

Configuring SSH and HTTPS

Complete the following steps to configure a management policy for SSH and HTTPS on the router.

Step 1   Click **Configure > Additional Tasks > Router Access > Management Access**.

Step 2   If there is no management policy, click **Add**. If you want to edit an existing management policy, select the policy and click **Edit**.

>✎
>**Note**   If you are editing a management policy it must be associated with an interface that has a static IP address.

Step 3   In the displayed dialog, enter the address information in the Source Host/Network box. The IP address information that you enter must include the IP address of the PC you will use to manage the router.

Step 4   Choose an outside interface with a static IP address in the Management Interface box. This interface must have a route to the IP address you specified in the Source Host/Network box.

Step 5   In the Management Protocols box, check **Allow SDM**.

Step 6   Check **HTTPS** and **SSH** to allow those protocols.

Step 7   Click OK to close the dialog.

Step 8   Click **Apply Changes** in the window that displays management access policies.

How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I View Activity on My Firewall?

Activity on your firewall is monitored through the creation of log entries. If logging is enabled on the router, whenever an access rule that is configured to generate log entries is invoked—for example, if a connection were attempted from a denied IP address—then a log entry is generated and can be viewed in Monitor mode.

Enable Logging

The first step to viewing firewall activity is to enable logging on the router. To enable logging:

Step 1   From the left frame, select **Additional Tasks.**

Step 2   In the Additional Tasks tree, click **Logging** and then click the **Edit** button.

Step 3   In the Syslog screen, check **Logging to Buffer**.

Step 4   In the Buffer Size field, enter the amount of router memory that you want to use for a logging buffer. The default value is 4096 bytes. A larger buffer will store more log entries but you must balance your need for a larger logging buffer against potential router performance issues.

Step 5   Click **OK**.

Identify the Access Rules for Which You Want to Generate Log Entries

In addition to enabling logging, you must identify the access rules that you want to generate log entries. To configure access rules for generating log entries:

Step 1   From the left frame, select **Additional Tasks.**

Step 2   In the Additional Tasks tree, click **ACL Editor**, and then click **Access Rules**.

Each access rule appears in the upper table on the right side of the screen. The lower table shows the specific source and destination IP addresses and the services that are permitted or denied by the rule.

Step 3   In the upper table, click the rule that you want to modify.

Step 4   Click **Edit**.

The Edit a Rule dialog box appears.

Step 5   The Rule Entry field shows each of the source IP/destination IP/service combinations that are permitted or denied by the rule. Click the rule entry that you want to configure to generate log entries.

Step 6   Click **Edit**.

Step 7   In the rule entry dialog box, check the **Log Matches Against this Entry** check box.

Step 8   Click **OK** to close the dialog boxes you have displayed.

The rule entry that you just modified will now generate log entries whenever a connection is attempted from the IP address range and services that the define the rule entry.

Step 9   Repeat Step 4 through Step 8 for each rule entry that you want to configure to generate log entries.

Once your logging configuration is complete, follow the steps below to view your firewall activity:

Step 1   From the toolbar, select **Monitor Mode**.

Step 2   From the left frame, select **Firewall Status**.

In the Firewall statistics, you can verify that your firewall is configured and view how many connection attempts have been denied.

The table shows each router log entry generated by the firewall, including the time and the reason that the log entry was generated.

How Do I Configure a Firewall on an Unsupported Interface?

Cisco SDM can configure a firewall on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. For more information on how to configure an interface using the CLI, refer to the Software Configuration Guide for your router.

To verify that the connection is working, verify that the interface status is "Up" in the Interfaces and Connections window.

The following is an exerpt showing the configuration for an ISDN interface on a Cisco 3620 router:

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
!  This is the data BRI WIC
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 100.100.100.100 name junky 883531601
 dialer hold-queue 10
 isdn switch-type basic-5ess
 isdn tei-negotiation first-call
 isdn twait-disable
 isdn spid1 80568541630101 6854163
 isdn incoming-voice modem
```

Other configurations are available in the Software Configuration Guide for your router.

After you have configured the unsupported interface using the CLI, you canuse Cisco SDM to configure the firewall. The unsupported interface will appear as "Other" in the fields listing the router interfaces.

How Do I Configure a Firewall After I Have Configured a VPN?

If a firewall is placed on an interface used in a VPN, the firewall must permit traffic between the local and remote VPN peers. If you use the Basic or Advanced Firewall wizard, Cisco SDM will automatically permit traffic to flow between VPN peers.

If you create an access rule in the ACL Editor available in Additional Tasks, you have complete control over the permit and deny statements in the rule, and you must ensure that traffic is permitted between VPN peers. The following statements are examples of the types of statements that should be included in the configuration to permit VPN traffic:

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

How Do I Permit Specific Traffic Through a DMZ Interface?

Follow the steps below to configure access through your firewall to a web server on a DMZ network:

Step 1   From the left frame, select **Firewall and ACL.**

Step 2   Select **Advanced Firewall**.

Step 3   Click **Launch the Selected Task**.

Step 4   Click **Next**.

The Advanced Firewall Interface Configuration screen appears.

Step 5   In the Interface table, select which interfaces connect to networks inside your firewall and which interfaces connect to networks outside the firewall.

Step 6   From the DMZ Interface field, select the interface that connects to your DMZ network.

Step 7   Click **Next>**.

Step 8   In the IP Address field, enter the IP address or range of IP addresses of your web server(s).

Step 9   From the Service field, select TCP.

Step 10   In the Port field, enter **80** or **www**.

Step 11   Click **Next>**.

Step 12   Click **Finish**.

How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?

You can use the Edit Firewall Policy tab to modify your firewall configuration to permit traffic from a new network or host.

Step 1   From the left frame, select **Firewall and ACL**.

Step 2   Click the **Edit Firewall Policy** tab.

Step 3   In the traffic selection panel select a From interface and a To interface to specify the traffic flow to which the firewall has been applied, and click **Go**. A firewall icon will appear in the router graphic if a firewall has been applied to the traffic flow. If the traffic flow you select does not display the access rule you need to modify, select a different From interface or a different To interface.

Step 4   Examine the access rule in the Service area. Use the **Add** button to disp.lay a dialog for a new access rule entry.

Step 5   Enter a permit statement for the network or host you want to allow access to the network. Click **OK** in the rule entry dialog.

Step 6   The new entry appears in the service area..

Step 7   Use the **Cut** and **Paste** buttons to reorder the entry to a different position in the list if you need to do so.

How Do I Configure NAT on an Unsupported Interface?

Cisco SDM can configure Network Address Translation (NAT) on an interface type unsupported by Cisco SDM. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is "Up."

After you have configured the unsupported interface using the CLI, you can configure NAT . The unsupported interface will appear as "Other" on the router interface list.

How Do I Configure NAT Passthrough for a Firewall?

If you have configured NAT and are now configuring your firewall, you must configure the firewall so that it permits traffic from your public IP address. To do this you must configure an ACL. To configure an ACL permitting traffic from your public IP address:

Step 1   From the left frame, select **Additional Tasks**.

Step 2   In the Rules tree, select **ACL Editor** and then **Access Rules**.

Step 3   Click **Add**.

The Add a Rule dialog box appears.

Step 4   In the Name/Number field, enter a unique name or number for the new rule.

Step 5   From the Type field, choose **Standard Rule**.

Step 6   In the Description field, enter a short description of the new rule, such as "Permit NAT Passthrough."

Step 7   Click **Add**.

The Add a Standard Rule Entry dialog box appears.

Step 8   In the Action field, choose **Permit**.

Step 9   In the Type field, choose **Host**.

Step 10   In the IP Address field, enter your public IP address.

Step 11   In the Description field, enter a short description, such as "Public IP Address."

Step 12   Click **OK**.

Step 13   Click **OK**.

The new rule now appears in the Access Rules table.

How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?

In order to permit traffic through your firewall to a VPN concentrator, you must create or modify access rules that permit the VPN traffic. To create these rules:

Step 1   From the left frame, select **Additional Tasks**.

Step 2   In the Rules tree, select **ACL Editor** and then **Access Rules**.

Step 3   Click **Add**.

The Add a Rule dialog box appears.

Step 4   In the Name/Number field, enter a unique name or number for this rule.

Step 5   In the Description field, enter a description of the rule, such as "VPN Concentrator Traffic."

Step 6   Click **Add**.

The Add an Extended Rule Entry dialog box appears.

Step 7   In the Source Host/Network group, from the Type field, select **A Network**.

Step 8   In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN source peer.

Step 9   In the Destination Host/Network group, from the Type field, select **A Network**.

Step 10   In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN destination peer.

Step 11   In the Protocol and Service group, select **TCP**.

Step 12   In the Source port fields, select =, and enter the port number **1023**.

Step 13   In the Destination port fields, select =, and enter the port number **1723**.

Step 14   Click **OK**.

The new rule entry appears in the Rule Entry list.

Step 15   Repeat Step 7 through Step 15, creating rule entries for the following protocols and, where required, port numbers:

- Protocol **IP**, IP protocol **GRE**
- Protocol **UDP**, Source Port **500**, Destination Port **500**
- Protocol **IP**, IP Protocol **ESP**
- Protocol **UDP**, Source Port **10000**, Destination Port **10000**

Step 16   Click **OK**.

How Do I Associate a Rule with an Interface?

If you use the Cisco SDM Firewall wizard, the access and inspection rules that you create are automatically associated with the interface for which you created the firewall. If you are creating a rule in Additonal Tasks/ACL Editor, you can associate it with an interface from the Add or Edit a Rule window. If you do not associate it with an interface at that time, you can still do so later.

Step 1   Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.

Step 2   Select the interface that you want to associate a rule with, and click **Edit**.

Step 3   In the Association tab, enter the rule name or number in the Inbound or Outbound field in the Access Rule or Inspection Rule boxes. If you want the rule to filter traffic before it enters the interface, use the Inbound field. If you want the rule to filter traffic that has already entered the router, but may exit the router through the selected interface, use the Outbound field.

Step 4   Click **OK** in the Association tab.

Step 5   In the Access Rules or the Inspection Rules window, examine the Used By column to verify that the rule has been associated with the interface.

How Do I Disassociate an Access Rule from an Interface

You may need to remove the association between an access rule and an interface. Removing the association does not delete the access rule. You can associate it with other interfaces if you want. To remove the association between an access rule and an interface, perform the following steps.

Step 1   Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.

Step 2   Select the interface that you want to disassociate the access rule from.

Step 3   Click **Edit**.

Step 4   In the Association tab, find the access rule in the inbound or outbound field in the Access Rule box. The access rule may have a name, or a number.

Step 5   Click in the inbound or outbound field, and then click the button to the right.

Step 6   Click **None (clear rule association)**.

Step 7   Click **OK**.

How Do I Delete a Rule That Is Associated with an Interface?

Cisco SDM does not allow you to delete a rule that is associated with an interface; you must first remove the association between the rule and the interface, and then delete the access rule.

Step 1   Click **Interfaces and Connections** in the left panel and click the **Edit Interfaces and Connections** tab.

Step 2   Select the interface that you want to disassociate the rule from.

Step 3   Click **Edit**..

Step 4   In the Association tab, find the rule in the Access Rule box or the Inspect Rule box. The rule may have a name or a number.

Step 5   Find the rule in the association tab. **If it is an access rule,** click **None (clear rule association). If it is an Inspection rule, click None**.

Step 6   Click **OK**.

Step 7   Click **Rules** in the left frame. Use the Rules tree to go to the Access Rule or the Inspection Rule window.

Step 8   Select the rule that you want to remove, and click **Delete**.

How Do I Create an Access Rule for a Java List?

Inspection rules allow you to specify Java lists. A Java list is used to permit Java applet traffic from trusted sources. These sources are defined in an access rule that the Java List references. To create this kind of access rule, and use it in a Java list, do the following:

Step 1   If you are at the Inspection Rules window, and you have clicked **Java List**, click the button to the right of the Number field and click **Create a new rule (ACL) and select.** The Add a Rule window opens.

If you are at the Access Rules window, click **Add** to open the Add a Rule window.

Step 2   From the Add a Rule window, create a standard access rule that permits traffic from the addresses you trust. For example, if you wanted to permit Java applets from hosts 10.22.55.3, and 172.55.66.1, you could create the following access rule entries in the Add a Rule window:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

You can provide descriptions for the entries and a description for the rule.

You do not need to associate the rule with the interface to which you are applying the inspection rule.

Step 3   Click **OK** in the Add a Rule window.

Step 4   If you started this procedure from the Inspection Rules window, then click **OK** in the Java List window. You do not need to complete Step 5 and Step 6.

Step 5   If you started this procedure in the Access Rules window, go to the Inspection Rules window and select the inspection rule you want to create a Java list for, and click **Edit**.

Step 6   Check **http** in the Protocols column, and click **Java List**.

Step 7   In the Java List Number field, enter the number of the access list that you created. Click **OK**.

How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?

The Firewall wizard, lets you specify the traffic that you want to allow onto the DMZ. If you do not have a DMZ network, you can still permit specified types of outside traffic onto your network, using the Firewall Policy feature.

Step 1   Configure a firewall using the Firewall wizard.

Step 2   Click **Edit Firewall Policy/ACL**.

Step 3   To display the access rule you need to modify, select the outside (untrusted) interface as the From interface, and the inside (trusted) interface as the To interface. The access rule applied to inbound traffic on the untrusted interface is displayed.

Step 4   To allow a particular type of traffic onto the network that is not already allowed, click **Add** in the Service area.

Step 5   Create the entries you need in the rule entry dialog.You must click **Add** for each entry you want to create.

Step 6   The entries you create will appear in the entry list in the Service area.

Firewall Policy

The Firewall Policy feature lets you view and modify firewall configurations—access rules and CBAC inspection rules—in the context of the interfaces whose traffic they filter. Using a graphical representation of the router and its interfaces, you can choose different interfaces on the router and see whether an access rule or an inspection rule has been applied to that interface. You can also view the details of the rules displayed in the Edit Firewall Policy/ACL window.

Edit Firewall Policy/ACL

Use the Edit Firewall Policy/ACL window to view the access and inspection rules in a context that displays the interfaces the rules are associated with. Also use it to modify the access and inspection rules that are displayed.

Configure a Firewall Before Using the Firewall Policy Feature

Before using the Edit Firewall Policy/ACL window, you should perform the following tasks:

1. **Configure LAN and WAN interfaces**. You must configure the LAN and WAN interfaces before you can create a firewall. You can use the LAN and WAN wizards to configure connections for your router.

2. **Use the Firewall Wizard to configure a firewall and a DMZ**.The Firewall Wizard is the easiest way to apply access rules and inspection rules to the inside and outside interfaces you identify, and will allow you to configure a DMZ interface and specify the services that should be allowed onto the DMZ network.

3. **Come to the Firewall Policy window to edit the firewall policy you created**. After configuring LAN and WAN interfaces and creating a firewall, you can open this window and get a graphical representation of the policy in a traffic flow. You can view the access rule and inspection rule entries and make any necessary changes.

Use the Firewall Policy View Feature

After you have created the firewall, you can use the Firewall Policy View window to get a graphical view of the firewall in the context of the router interfaces, and to modify it if you need to.

For more information, click the action that you want to take:

- Choose a Traffic Flow
- Examine the Traffic Diagram and Choose a Traffic Direction
- Make Changes to Access Rules
- Make Changes to Inspection Rules

For a use case example, see Firewall Policy Use Case Scenario.

Note   If the router is using a Cisco IOS image that does not support the Firewall feature set, only the Services area will be displayed, and you will only be able to create access control entries.

Apply Changes Button

Click to deliver changes you have made in this window to the router. If you leave the Edit Firewall Policy/ACL window without clicking **Apply Changes**, Cisco SDM displays a message indicating that you must either apply changes or discard them.

Discard Changes Button

Click to discard changes you have made in this window. This button does not let you remove changes that you have delivered to the router using the **Apply Changes** button.

Choose a Traffic Flow

Traffic flow refers to traffic that enters the router on a specified interface (the *from* interface) and exits the router on a specified interface (the *to* interface). The Cisco SDM traffic-flow display controls are located in a row at the top of the Edit Firewall Policy/ACL window.

Note   There must be a least two configured interfaces on the router. If there is only one, Cisco SDM will display a message telling you to configure an additional interface.

The following table defines the Cisco SDM traffic-flow display controls.

From	Choose the interface from which the traffic flow you are interested in originates. The firewall will protect the network connected to the From interface. The **From** drop-down list contains only interfaces with configured IP addresses.
To	Choose the interface out of which the traffic will leave the router. The **To** drop-down list contains only interfaces with configured IP addresses.
	Details button. Click to view details about the interface. Details such as IP address, encapsulation type, associated IPSec policy, and authentication type are provided.
Go button	Click to update the traffic-flow diagram with information about the interfaces you have chosen. The diagram is not updated until you click **Go**. The **Go** button is disabled if you have not chosen a From interface or a To interface, or if the From and To interfaces are the same.
View Option	Choose **Swap From and To interface** to swap the interfaces that you originally chose in the **From** and **To** drop-down lists. You can use the swap option if you want to create a firewall protecting both the network connected to the From interface and the network connected to the To interface. You can choose **View all Access control lists in traffic flow** when one access rule has been applied to the From interface and another access rule has been applied to the To interface for a traffic direction you have chosen. The entries of both access rules are displayed in another window.

Cisco SDM displays interfaces that have IP addresses in alphabetical order in both the **From** and **To** drop-down lists. By default, Cisco SDM chooses the first interface in the **From** list, and the second interface in the **To** list. Use the **From** and **To** drop-down lists to choose a different traffic flow. The chosen traffic flow is displayed in the traffic diagram below the traffic-flow display controls.

For example, to view traffic flow from a network connected to the router interface Ethernet 0 and exiting on the router interface Serial 0, follow these steps:

Step 1   Choose Ethernet 0 in the **From** drop-down list.

Step 2   Choose Serial 0 in the **To** drop-down list.

Step 3   Click **Go**.

Step 4   To switch the interfaces in the **From** and **To** drop-down lists, choose **Swap From and To interface** from the View Option drop-down list.

Access rules applied to originating and returning traffic may be different. To learn more about how to switch between displaying originating and returning traffic in the traffic diagram, see Examine the Traffic Diagram and Choose a Traffic Direction.

Step 5   Click the **Details** button next to the **From** or **To** drop-down list to open a window showing an interface's IP address, IPSec policy, and other information.

To work with the traffic diagram, see Examine the Traffic Diagram and Choose a Traffic Direction. To return to the main Firewall Policy window description see Edit Firewall Policy/ACL.

Examine the Traffic Diagram and Choose a Traffic Direction

The traffic diagram displays the router with the chosen From and To interfaces (see Choose a Traffic Flow for more information). It also displays the types of rules applied for the chosen traffic flow, as well as the direction in which they have been applied.

Originating Traffic

Click to highlight the traffic flow that enters the router at the From interface and exits the router at the To interface. When this area is highlighted, you can see the details of rules applied in the direction of traffic flow.

Returning Traffic

Click to highlight the traffic flow that enters the router on the To interface and exits the router on the From interface. When this area is highlighted, you can see the details of rules applied to returning traffic.

Icons

Rules are represented by icons in the traffic flow:

	A filter symbol indicates that an access rule is being applied.
	A magnifying glass indicates that an inspection rule is being applied.
	A firewall icon in the router indicates that a firewall has been applied to the Originating traffic flow. Cisco SDM displays a firewall icon if the following sets of criteria are met: • There is an inspection rule applied to Originating traffic on the inbound direction of the From interface, and there is an access rule applied to the inbound direction of the To interface. • The access rule on the inbound direction of the To interface is an extended access rule, and contains at least one access rule entry. No firewall icon is displayed when a firewall has been applied to Returning traffic. If the Firewall feature is available, but no firewall has been applied to the traffic flow, **IOS Firewall: Inactive** will be displayed underneath the traffic diagram.

	Rules applied to Originating traffic are indicated by a right arrow. An icon on the From interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon placed on the To interface traffic line indicates a rule filtering traffic outbound from the router. If you place the mouse over this icon, Cisco SDM will display the names of the rules that have been applied.
	Rules applied to Returning traffic are indicated by a left arrow. An icon on the To interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon on the From interface traffic line indicates the presence of a rule filtering traffic outbound from the router. The names of the rules applied are displayed when you place the cursor over this icon.

Note   Although the icons are shown on a particular interface in the diagram, a firewall policy might contain access control entries that affect traffic not represented by the diagram. For example, an entry that contains the wildcard icon in the Destination column (see Make Changes to Access Rules) might apply to traffic exiting interfaces other than the one represented by the currently chosen To interface. The wildcard icon appears as an asterisk and stands for any network or host.

To make changes to an access rule, see Make Changes to Access Rules. To return to the main Firewall Policy window description see Edit Firewall Policy/ACL.

Make Changes to Access Rules

The policy panel shows the details of the rules applied to the chosen traffic flow. The Policy panel is updated when the From and To interfaces are chosen and when the Traffic Diagram is toggled between Originating Traffic focus and Returning Traffic focus.

The Policy panel is blank if an access rule that contains no entries has been associated with an interface. For example, if a rule name was associated with an interface using the CLI, but entries for the rule were not created, this panel would be blank. If the Policy Panel is blank, you can use the **Add** button to create entries for the rule.

Service Area Header Fields

Firewall Feature Availability	If the Cisco IOS image that the router is using supports the Firewall feature, this field contains the value **Available**.
Access Rule	The name or number of the access rule whose entries are being displayed.
Inspection Rule	The name of the inspection rule whose entries are being displayed.
⚠	This icon appears when an access rule has been associated with an interface, but no access rule of that name or number has been created. Cisco SDM informs you that the policy has no effect unless there is at least one access rule entry.

Service Area Controls

The following table describes the controls found in the Service Area.

Add button	Click to add an access rule entry. Specify whether you want to add the entry before or after the entry currently chosen. Then, create the entry in the Add an Entry window. Remember that the order of entries is important. Cisco SDM displays the Extended entry dialog when you add an entry from the Edit Firewall Policy/ACL window. To add a standard rule entry, go to **Additional Tasks > ACL Editor > Access Rules**.
Edit button	Click to edit a chosen access rule entry. Although you can only add extended rule entries in the Edit Firewall Policy/ACL window, you are not prevented from editing a standard rule entry that has already been applied to a chosen interface.

Cut button	Click to remove a chosen access rule entry. The entry is placed on the clipboard and can be pasted to another position in the list, or it can be pasted to another access rule. If you want to reorder an entry, you can cut the entry from one location, choose an entry before or after the location that you want for the cut entry, and click **Paste**. The Paste context menu allows you to place the entry before or after the entry you chose.
Copy button	Choose a rule entry and click to put the rule entry on the clipboard.
Paste button	Click to paste an entry on the clipboard to the chosen rule. You will be prompted to specify whether you want to paste the entry before or after the currently chosen entry. If Cisco SDM determines that an identical entry already exists in the access rule, it displays the Add an Extended Rule Entry window so that you can modify the entry. Cisco SDM does not allow duplicate entries in the same access rule.
Interface drop-down list	If the chosen traffic flow (Originating or Returning) contains an access rule on both the From interface and the To interface, you can use this list to toggle between the two rules.
Apply Firewall	If the chosen traffic flow does not have a firewall applied, you can apply a firewall by choosing Originating traffic and clicking the Apply Firewall button. By default, clicking Apply Firewall will associate an Cisco SDM-default inspection rule to the inbound direction of the From interface, and will associate an access rule to the inbound direction of the To interface that denies traffic. If the Cisco IOS image that the router is using does not support the Firewall feature, this button is disabled. For example, to apply a firewall that protects the network connected to the **Ethernet 0** interface from traffic entering the Ethernet 1 interface, choose Ethernet 0 from the **From** drop-down list, and Ethernet 1 from the **To** drop-down list. Then click **Apply Firewall**. If you want to apply a firewall that protects the network connected to the Ethernet 1 interface from traffic entering the Ethernet 0 interface, go to **Additional Tasks > ACL Editor > Access Rules**.

Service area buttons are disabled if the rule is read-only. A rule is read-only when it contains syntax that Cisco SDM does not support. Read-only rules are indicted by this icon: .

If there is an existing standard rule that filters the returning traffic flow to which you are applying the firewall, Cisco SDM informs you that it will convert the standard access rule to an extended rule.

Service Area Entry Fields

The following table describes the icons and other data in the Service Area entries.

Field	Description	Icons	Meaning
Action	Whether the traffic will be permitted or denied		Permit source traffic
			Deny source traffic
Source/ Destination	Network or host address, or any host or network.		The address of a network
			The address of a host
			Any network or host
Service	Type of service filtered.	IP	Examples: TCP, EIGRP, UDP, GRE. See IP Services.
		TCP	Examples: Telnet, http, FTP. See TCP Services.
		UDP	Examples: SNMP, bootpc, RIP. See UDP Services.
		IGMP	Internet Group Management Protocol (IGMP).
		ICMP	Examples: echo-reply, host-unreachable. See ICMP Message Types.
Log	Whether or not denied traffic is logged.		Log denied traffic. To configure logging for firewalls see Firewall Log.

Field	Description	Icons	Meaning
Option	Options configured using the CLI	No icons.	
Description	Any description provided.	No icons	

To make changes to inspection rules, see Make Changes to Inspection Rules. To return to the main Firewall Policy window description see Edit Firewall Policy/ACL.

Make Changes to Inspection Rules

The Applications area appears if the Cisco IOS image running on the router supports CBAC Inspection rules. The Applications area displays the inspection rule entries that are filtering the traffic flow, and is updated whenever a new traffic flow is chosen. The inspection rule that affects the chosen direction of traffic is displayed.

The Applications area will display one of the following for **Originating traffic**:

- The inspection rule that is applied to the inbound direction of the From interface, if one exists.
- The inspection rule that is applied to the outbound direction of the To interface, if the inbound direction of the From interface has no inspection rule applied.

Swap From and To Interfaces to Bring Other Rules into View

Inspection rules applied to **Returning traffic** are not displayed.You can display an inspection rule applied to **Returning traffic** by choosing **Swap From and To interfaces** in the View Options menu. You can also view inspection rules that are not displayed in the Edit Firewall Policy/ACL window by going to the Application Security window in the Firewall and ACL task.

⚠   This icon appears when two inspection rules are found in the chosen traffic direction. Cisco SDM also displays a warning dialog, giving you the opportunity to dissociate one of the inspection rules from the interface.

Application Area Controls

The following is a list of Application area controls:

Add—Click to add an inspection rule. If there is no inspection rule, you can add the Cisco SDM default inspection rule, or you can create and add a custom inspection rule. If you add the Cisco SDM default inspection rule to a traffic flow with no inspection rule, it will be associated with the inbound traffic to the From interface. You can add an entry for a specific application whether or not an inspection rule already exists.

Edit—Click to edit a chosen entry.

Delete—Click to delete a chosen entry.

Global Settings—Click to display a dialog box that enables you to set global timeouts and thresholds.

Summary—Click to display the application or protocol name and a description for each entry.

Detail—Click to display the application or protocol name, description, alert status, audit trail status, and timeout settings for each entry.

Application Area entry fields

The following list describes the Application area entry fields:

Application Protocol—Displays the name of the application or protocol. For example, **vdolive**.

Alert—Indicates whether or not an alert is on (default) or off.

Audit Trail—Indicates whether or not audit trail is on or off (default).

Timeout—Displays how long, in seconds, the router waits before blocking return traffic for this protocol or application.

Description—Displays a short description. For example, **VDOLive protocol**.

To return to the main Firewall Policy window description see Edit Firewall Policy/ACL.

Add *App-Name* Application Entry

Use this window to add an application entry that you want the Cisco IOS firewall to inspect.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value for the protocol or application.

Add rpc Application Entry

Add a Remote Procedure Call (RPC) program number in this window, and specify Alert, Audit, Timeout, and Wait time settings.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.

- **on**—Enable alert.

- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.

- **on**—Enable audit trail.

- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Program Number

Enter a single program number in this field.

Wait Time

You can optionally specify how many minutes to allow subsequent RPC connections from the same source to be made to the same destination address and port. The default wait time is zero minutes.

Add Fragment application entry

In this window, you can add a fragment entry to an inspection rule that you are configuring in the Edit Firewall Policy/ACL window, and you can specify Alert, Audit, and Timeout settings. A fragment entry sets the maximum number of unreassembled packets that the router should accept before dropping them.

Alert Action

Choose one of the following:

- **default(on)**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default(off)**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Range (optional)

Enter the maximum number of unreassembled packets the router should accept before dropping them. The range can have a value between 50 and 10000.

Add or Edit http Application Entry

Use this window to add an http application to the inspection rule.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.

- **on**—Enable audit trail.

- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Hosts/network for Java applet download

The source hosts or networks whose applet traffic is to be inspected. Multiple hosts and networks can be specified.

Click **Add** to display the Java Applet Blocking window in which you can specify a host or network.

Click **Delete** to remove an entry from the list.

Java Applet Blocking

Use this window to specify whether Java applets from a specified network or host should be permitted or denied.

Action

Choose one of the following:

- **Do Not Block (Permit)**—Permit Java applets from this network or host.

- **Block (Deny)**—Deny Java applets from this network or host.

Host/Network

Specify the network or the host.

Type

Choose one of the following:

- **A Network**—If you choose this, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.

- **A Host Name or IP Address**—If you choose this, provide a host IP address or host name in the next field.

- **Any IP address**—If you choose this, the action you specified is to apply to any host or network.

IP Address/Wildcard Mask

Enter a network address and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any Java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any Java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you chose **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network that can resolve the host name to an IP address.

Cisco SDM Warning: Inspection Rule

This window is displayed when Cisco SDM finds two inspection rules have been configured for a direction in a traffic flow. For example, you might have one inspection rule applied to traffic inbound on the From interface, and another applied to traffic outbound on the To interface. Two inspection rules may not harm the functioning of the router, but they may be unnecessary. Cisco SDM allows you to keep the inspection rules the way they are, to remove the inspection rule on the From interface, or to remove the inspection rule on the To interface.

- **Do not make any change**—Cisco SDM will not remove either inspection rule.

- **Keep inspection rule** *name* **on <**interface-name**> inbound, and dissociate inspection rule** *name* **on <**interface-name**> outbound**—Cisco SDM will keep one inspection rule, and dissociate the rule from the other interface.

- **Keep inspection rule** *name* **on <**interface-name**> outbound and dissociate inspection rule** *name* **on <**interface-name**> inbound**—Cisco SDM will keep one inspection rule, and dissociate the rule from the other interface.

Before you make a selection and click **OK**, you may want to click **Cancel**, then determine if you need to add entries to the inspection rule you want to retain. You can add entries by using the **Add** button in the Application area toolbar in the Edit Firewall Policy/ACL window.

Cisco SDM Warning: Firewall

This window appears when you click **Apply Firewall** in the Edit Firewall Policy/ACL window. It lists the interfaces to which it will apply a rule, and describes the rule that it will apply.

Example:

```
SDM will apply firewall configuration to the following interfaces:
Inside (Trusted) Interface: FastEthernet 0/0
* Apply inbound default SDM Inspection rule
* Apply inbound ACL. Anti-spoofing, broadcast, local loopback, etc.).

Outside (Untrusted) Interface: Serial 1/0
* Apply inbound access list to deny returning traffic.
```

Click **OK** to accept these changes, or click **Cancel** to stop the application of the firewall.

Edit Firewall Policy

The Edit Firewall Policy window provides a graphical view of the firewall policies on the router and enables you to add ACLs to policies without leaving the window. Read the procedures in the sections that follow to see how to view the information in this window and add rules.

This help topic contains the following sections:

- Things You Must do Before Viewing Information in this Window

- Expanding and Collapsing the Display of a Policy
- Adding a New Rule to a Policy
- Adding a New Zone Policy
- Reordering Rules Within a Policy
- Copying and Pasting a Rule
- Displaying the Rule Flow Diagram
- Applying Your Changes
- Discarding Your Changes

Things You Must do Before Viewing Information in this Window

This window is empty if no zone, zone-pairs, or policy maps have been configured. Create a basic configuration containing these elements by going to **Configure > Firewall and ACL > Create Firewall** and completing the Advanced Firewall wizard. After you have done this, you can create additional zones, zone pairs and policies as needed by going to **Configure > Additional Tasks > Zones** to configure zones, and to **Additional Tasks > Zone Pairs** to configure additional zone pairs.

To create the policy maps that the zone pairs are to use, go to **Configure > Additional Tasks > C3PL**. Click the **Policy Map** branch to display additional branches which enable you to create policy maps and the class maps that define traffic for the policy maps.

Expanding and Collapsing the Display of a Policy

When the display of a policy is collapsed, only the policy name and the source and destination zones are displayed. To expand the display of the policy to show the rules that make up the policy, click the **+** button to the left of the policy name. An expanded view of a firewall policy might look similar to the following:

	Traffic Classification			Action	Rule Options
ID	Source	Destination	Service		
clients-servers-policy (clients to servers)					
1	any	any	tcp	Permit Firewall	

		Traffic Classification		Action	Rule Options
			udp		
			icmp		
2	Unmatched Traffic			Drop	

The policy named clients-servers-policy contains two ACLs. The rule with the ID 1 permits TCP, UDP, and ICMP traffic from any source to any destination. The rule with the ID 2 drops any unmatched traffic.

Adding a New Rule to a Policy

To add a new rule to a policy, complete the following steps:

Step 1   Click anywhere in the display for that policy, and click the **+ Add** button.

- To insert a rule for new traffic in the order that you want it select an existing rule, click the **+ Add** button, and choose **Insert** or **Insert After**. The Insert and Insert After options are also available from a context menu that you display by right-clicking on an existing rule.

- Choosing **Rule for New Traffic** automatically places the new rule at the top of the list.

- Choosing **Rule for Existing** Traffic allows you to select an existing class map and modify it. It automatically places the new rule at the top of the list.

Step 2   Complete the displayed dialog. Click Add a New Rule for more information.

Adding a New Zone Policy

To add a new zone policy, complete the following steps:

Step 1   Click Add and choose New Zone Policy.

Step 2   In the Add a Rule screen, specify the source zone by clicking the button to the right of the Source Zone field and selecting an existing zone or creating a new zone.

Step 3 Specify the destination zone by clicking the button to the right of the Destination Zone field and selecting an existing zone or creating a new zone.

Make settings in the other fields of the Add a Rule window. See Add a New Rule for more information.

Reordering Rules Within a Policy

If a policy contains more than one rule that permits traffic, you can reorder them by selecting a rule and clicking the **Move Up** button or the **Move Down** button. The Move Up button is disabled if you selected a rule that is already at the top of the list, or if you selected the Unmatched Traffic rule. The Move Down button is disabled if you selected a rule that is already at the bottom of the list.

You can also use the Cut and the Paste buttons to reorder rules. To remove a rule from its current position, select it and click **Cut**. To place the rule in a new position, select an existing rule, click **Paste**, and choose **Paste** or **Paste After**.

The Move Up, Move Down, Cut, Paste, and Paste After operations are also available from the context menu displayed when you right-click on a rule.

Copying and Pasting a Rule

Copying and pasting a rule is very useful if one policy contains a rule that can be used with few or no modifications in another policy.

To copy a rule, select a rule and click the **Copy** button or right-click the rule and choose **Copy**. To paste the rule to a new location, click **Paste** and choose **Paste** or **Paste After**. The Paste and Paste After buttons are also available from the context menu. When you paste a rule to a new location, the Add a New Rule dialog is displayed so you can make changes to the rule if you need to.

Displaying the Rule Flow Diagram

Click anywhere in a firewall policy and click Rule Diagram to display the Rule Flow Diagram for that policy. The Rule Flow Diagram displays the source zone on the right of the router icon, and the destination zone on the left of the icon.

Applying Your Changes

To send your changes to the router, click **Apply Changes** at the bottom of the screen.

Discarding Your Changes

To discard changes that you have made but have not sent to the router, click **Discard Changes** at the bottom of the screen.

Add a New Rule

Define a traffic flow and specify protocols to inspect in the Add a Rule window. Complete the following steps to add a new rule.

Step 1   If you are creating a zone policy, the Source Zone and Destination Zone fields appear. Do the following:

   a.   To specify the source zone, click the button next to the Source Zone field. To choose an existing zone click **Select a Zone** and choosing the zone from the displayed dialog. To create a zone, click **Create a Zone**, enter a zone name, and specify the interfaces to associate with the zone in the displayed dialog.

   b.   To specify the destination zone, click the button next to the Destination Zone field. To choose an existing zone click **Select a Zone** and choosing the zone from the displayed dialog. To create a zone, click **Create a Zone**, enter a zone name, and specify the interfaces to associate with the zone in the displayed dialog.

Step 2   In the Source and Destination field, specify that the traffic is flowing between a network and another network by choosing **Network**, or that the traffic is flowing between entities that may be networks or may be individual hosts by choosing **Any**.

Step 3   Enter a name for the traffic flow in the Traffic Name field.

Step 4   Click **Add** next to the Source Network and Destination Network columns and add source and destination network addresses. You can add multiple entries for the source and destination networks, and you can edit an existing entriy by selecting it and clicking **Edit**.

Step 5   Reorder an entry if necessary by selecting it and clicking **Move Up** or **Move Down**. The Move Up button is disabled when the selected entry is already at the top of the list. The Move Down button is disabled when the selected entry is already at the bottom of the list.

Step 6   Enter a name that describes the protocols or services that you are identifying for inspection in the Service Name field.

Step 7   To specify a service click on a branch in the tree in the left-hand column, choose the service, and click **Add>>**. Click the **+** icon next to a branch to display the available services of that type. To remove a service from the right-hand column, select it and click **<<Remove**.

Step 8   To specify how you want the traffic handled, choose **Permit Firewall**, **Permit ACL**, or **Drop** in the Action field. If you choose **Permit Firewall**, you can click Advanced and choose a menu item if you want to further define the action, such as inspecting the protocols that you chose in the service box. See the following help topics for more information:

- Application Inspection
- URL Filter
- Quality of Service
- Inspect Parameter

Step 9   If you chose **Drop** as the action, you can click **Log** to have the event logged.

Step 10   Click OK to close this dialog and send the changes to the router.

Add Traffic

Use the Add Traffic dialog to create a source and destination address entry for a rule.

Action

Use the Include or the Exclude option to specify whether you want the rule to apply to the traffic exchanged between the source and destination addresses.

Choose **Include** to include this traffic in the rule.

Choose **Exclude** to have this traffic excluded from the rule.

Source Host/Network and Destination Host/Network

Specify the source and the destination of the traffic in these fields.

Type

Choose one of the following values:

- Any IP Address—Choose if you do now want to limit the source or destination traffic to any host or network.

- A Network—Choose if you want to specify a network address as the source or destination, and specify the network address in the IP Address and Wildcard Mask fields.

- A Host Name or IP Address—Choose if you want to specify the name or IP address of a host. Then, specify the host in the Host Name/IP field.

IP Address

Enter the network address. This field is displayed when you choose **A Network** in the Type field.

Wildcard Mask

Enter the wildcard mask that specifies the bits that are used for the network address. For example, if the network address is 192.168.3.0, specify 0.0.0.255 as the mask. This field is displayed when you choose **A Network** in the Type field.

Host Name/IP

Enter the name or the IP address of a host in this field. If you enter a name, the router must be able to contact a DNS server to resolve the name to an IP address. This field is displayed whenyou choose A Host Name or IP Address in the Type field.

Application Inspection

Configure deep packet inspection for any of the applications or protocols listed in this screen by checking the box next to the application or protocol, clicking the button to the right of the field, and choosing **Create** or **Select** from the context menu. Choose **Create** to configure a new policy map. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.

For example, to create a new policy map for Instant Messaging, check the box next to IM, click the button next to the IM field, and choose **Create**. Then, create the policy map in the Configure Deep Packet Inspection dialog.

URL Filter

Add an URL filter by choosing an existing URL filter from the URL Filter Name list, or by clicking **Create New** and making a new URL filter in the dialogs displayed. the settings for the URL filter that you chose or created are summarized in this dialog.

Quality of Service

You can drop traffic that exceeds a specified rate per second, the police rate, and drop traffic that exceeds a specified burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The burst rate can be a value between 1,000 and 512,000,000 bytes.

Inspect Parameter

Specify an existing parameter map in the Inspect Parameter window by choosing a parameter map in the Inspect Parameter Map list, or click **Create New** to create a new parameter map to apply to the rule for the policy you are modifying. The details of the parameter map that you specify are displayed in the Preview box.

To learn about parameter maps, click Timeouts and Thresholds for Inspect Parameter Maps and CBAC.

Select Traffic

Select a class map that specifies the traffic that you want to add to the policy. To view more information about a particular class map, select the class map and click **View Details**.

When you click **OK**, the Add a New Rule dialog is displayed, with the information in the class map that you chose. You can make additional changes to the class map or leave it unchanged. If you do make changes, you can change the name of the class map if you do not want your changes to apply to other policies that use the original class map.

Delete Rule

This dialog is displayed when you delete a rule that contains a class map or ACL that you might want to delete along with the rule or keep for use in other rules.

Automatically delete class maps and ACLs used by this rule

Click this option to remove the class maps and ACLs that are part of this rule. They will be removed from the router configuration and not be available for use by other rules.

I will delete the unused class maps and ACLs later

Click this option to remove the rule but retain the class maps and ACLs. You can keep them for use in other parts of the firewall configuration.

View Details

Click **View Details** to display the names of the class maps and ACLs that are associated with the rule you are deleting. The dialog expands to show the details.When you click View Details, the button name becomes Hide Details.

Hide Details

Click **Hide Details** to close the details portion of the dialog. When you click Hide Details, the button name becomes View Details.

Manually Deleting Class Maps

To manually delete a class map, complete the following steps.

Step 1   Go to **Configure > Additional Tasks** > **C3PL > Class Maps**.

Step 2   Click the node for the type of class map that you are deleting.

Step 3   Select the name of the class map that was displayed in the View Details window and click **Delete**.

Manually Deleting ACLs

To manually delete an ACL, complete the following steps.

Step 1   Go to **Configure > Additional Tasks > ACL Editor**.

Step 2   Click the node for the type of ACL that you are deleting.

Step 3   Select the name or number of the ACL that was displayed in the View Details window and click **Delete**.

Application Security

Application Security allows you to create security policies to govern the use of network and web applications. You can apply the policies that you create to specific interfaces, clone an existing policy to leverage the settings for a new policy, and remove policies from the router.

This chapter contains the following sections:

- Application Security Windows
- No Application Security Policy
- E-mail
- Instant Messaging
- Peer-to-Peer Applications
- URL Filtering
- HTTP
- Applications/Protocols
- Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Application Security Windows

The controls in the Application Security windows allow you to associate policies with interfaces, make global settings, and add, delete and clone application security policies. The application security drawers enable you to quickly navigate to the application security area in which you need to make changes.

Policy Name List

Select the policy that you want to modify from this list. If no policies are configured, this list is empty, and the Application Security window displays a message that indicates no policies are available on the router. To create a policy, click the **Action** button, and choose **Add**.

Application Security Buttons

- **Action** button—Click to add a policy, delete the chosen policy, or clone the chosen policy. If no policies are configured on the router, **Add** is the only action available.

- **Associate** button—Click to display a dialog that allows you to associate the policy with an interface. The dialog enables you to choose the interface, and to specify the traffic direction to which the policy is to apply.

- **Global Settings** button—Click to make settings to timeout and threshold values that apply to all policies. Click Global Settings for more information.

E-mail Drawer

Click to make changes to e-mail application security settings. Click E-mail for more information.

Instant Messaging Drawer

Click to make changes to security settings for Yahoo Messenger, MSN Messenger, and other instant messaging applications. Click Instant Messaging for more information.

Peer-to-Peer Drawer

Click to make changes to security settings for KaZa A, eDonkey, and other peer-to-peer applications. Click Applications/Protocols for more information.

URL Filtering Drawer

Click to add a list of URLs that you want the application security policy to filter. You can also add filtering servers.

HTTP Drawer

Click to make changes to HTTP security settings. Click HTTP for more information.

Applications/Protocols Drawer

Click to make changes to the security settings of other applications and protocols. Click Applications/Protocols for more information.

No Application Security Policy

Cisco SDM displays this window when you click the **Application Security** tab, but no Application Security policy is configured on the router. You can create a policy from this window, and view the global settings that provide default values for the parameters that you can set when you create policies.

Policy Name

Empty when no policy is configured for the router. Choosing Add from the Action context menu enables you to create a policy name and to begin to make settings for the policy.

Action

If no policy is configured on the router, you can choose **Add** from the context menu to create a policy. Once a policy is configured, the other actions, **Edit** and **Delete**, are available.

Associate

If no policy is configured this button is disabled. When a policy is created, you can click this button to associate the policy with an interface. See Associate Policy with an Interface for more information.

Global Settings

Global settings provide the default timouts, thresholds, and other values for policy parameters. Cisco SDM provides defaults for each parameter, and you can change each value to define a new default that will apply unless overridden for a specific application or protocol. When you are creating a policy, you can accept the default value for a particular parameter, or choose another setting. Because the Application Security configuration windows do not display the default values you must click this button to view them in the Global Timeouts and Thresholds window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

E-mail

Specify the e-mail applications that you want to inspect in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Edit Button

Click to edit the settings for the chosen application. Settings that you create override the global settings configured on the router.

Applications Column

The name of the e-mail application, for example *bliff*, *esmtp*, and *smtp*. To edit the settings for an application, check the box to the left of the application name, and click **Edit**.

Alerts, Audit, and Timeout Columns

These columns display values that have been explicitly set for an application. If a setting is not changed for an application, the column is empty. For example, if auditing has been enabled for the bliff application, but no changes have been made to the alert or to the timeout settings, the value *on* is displayed in the **Audit** column, and the **Alert** and **Timeout** columns are blank.

Options Column

This column can contain fields if other settings for the chosen application exist.

MAX Data Field

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login Checkbox

Causes a user at a nonsecure location to use encryption for authentication.

Reset

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Instant Messaging

Use this window to control the traffic for Instant Messaging (IM) applications such as Yahoo Messenger, and MSN Messenger. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for Yahoo Messenger traffic, and alarms generated when traffic for that application arrives:

```
Yahoo Messenger      Block          Send Alarm (checked)
```

The SDM_HIGH profile blocks IM applications. If the router uses the SDM_HIGH profile, and it does not block IM applications, those applications may have connected to a new server that is not specified in the profile. To enable

the router to block these applications, check the **Send Alarm** checkbox next to the IM applications to reveal the names of the servers to which the applications connect. Then, use the CLI to block traffic from these servers. The following example uses the server name newserver.yahoo.com:

```
Router(config)# appfw policy-name SDM_HIGH
Router(cfg-appfw-policy)# application im yahoo
Router(cfg-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
Router(cfg-appfw-policy-ymsgr)# exit
Router(cfg-appfw-policy)# exit
Router(config)#
```

Note
- IM applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco SDM configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.

- Some IM applications, such as MSN Messenger 7.0, use HTTP ports by default. To permit these applications, configure the IM application to use its native port.

Peer-to-Peer Applications

This page allows you to create policy settings for peer-to-peer applications such as Gnutella, BitTorrent, and eDonkey. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for BitTorrent traffic, and alarms generated when traffic for that application arrives:

Example 10-1   Blocking BitTorrent Traffic

```
BitTorrent          Block
```

Note
- Peer-to-peer applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco SDM configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.

- Application security policies will not block files if they are being provided by a paid service such as altnet.com. Files downloaded from peer-to-peer networks are blocked.

URL Filtering

URL filtering allows you to control user access to Internet websites by using URL lists. In these lists, you can specify whether a URL is to be permitted or denied. Include URL filtering capabilities in the Application Security policy by clicking **Enable URL filtering** in this window.

You can configure one local URL list on the router that is used for all Application Security policies. URL lists can also be stored on URL filter servers that the router can connect to. Information for these servers is stored in a URL filter server list. You can configure one URL filter server list on the router that is used for all Application Security policies.

The local URL list can be maintained in this window by using the **Add URL**, **Edit URL**, and **Import URL list** buttons. Because Cisco IOS software can maintain these lists with or without a configured Application Security policy, you can also maintain these lists the Additional Tasks window.

To learn how to maintain a local URL list, click Local URL List.

To learn how to maintain the URL filter server list, click URL Filter Servers.

For information on how the router uses a local URL list in combination with URL lists on URL filter servers, click URL Filtering Precedence.

For general information about URL filtering, click URL Filtering Window.

HTTP

Specify general settings for HTTP traffic inspection in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes when it encounters traffic with the characteristics that you specify in this window.

For more detailed information about how the router can inspect HTTP traffic, see *HTTP Inspection Engine* at the following link:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455acb.html

Detect noncompliant HTTP traffic Checkbox

Check if you want Cisco SDM to examine HTTP traffic for packets that do not comply with the HTTP protocol. Use the Permit, Block, and Alarm controls to specify the action that the router takes when this type of traffic is encountered.

Note Blocking noncompliant HTTP traffic can cause the router to drop traffic from popular websites that might not be blocked on the basis of content, if those websites do not conform to the HTTP protocol.

Detect tunneling applications Checkbox

Check if you want Cisco SDM to examine HTTP traffic for packets that are generated by tunneling applications. Use the Permit, Block, and Alarm controls to specify the action that you want Cisco SDM to take when it encounters this type of traffic.

Set maximum URI length inspection Checkbox

Check if you want to define a maximum length for Universal Resource Indicators (URIs). Specify the maximum length in bytes, and then use the Permit, Block, and Alarm controls to specify the action that the router takes if it encounters an URL that is longer than this value.

Enable HTTP inspection Checkbox

Check if you want the router to inspect HTTP traffic. If you want to block traffic from Java applications, you can specify a Java blocking filter by clicking the ... button and either specifying an existing ACL, or creating a new ACL for Java inspection.

Enable HTTPS inspection checkbox

Check if you want the router to inspect HTTPS traffic.

Set time out value checkbox

Check if you want to set a time out for HTTP sessions, and enter the number of seconds in the Time-Out field. Sessions will be dropped that exceed this amount of time.

Enable audit trail

You can make CBAC audit trail settings for HTTP traffic that will override the setting in the Global Timeouts and Thresholds window. **Default** means that the current global setting will be used. **On** explicitly enables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting. **Off** explicitly disables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting.

Header Options

You can have the router permit or deny traffic based on HTTP header length and the request method contained in the header. Request methods are the commands sent to HTTP servers to fetch URLs, web pages, and perform other actions. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Set maximum header length checkbox

> Check if you want the router to permit or deny traffic based on HTTP header length, and specify the maximum Request and maximum Response header length. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if header length exceeds these lengths.

Configure Extension Request Method checkboxes

> If you want the router to permit or deny HTTP traffic based on an extension request method, check the box next to that request method. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if it encounters traffic using that request method.

Configure RFC Request Method checkboxes

> If you want the router to permit or deny HTTP traffic based on one of the HTTP request methods specified in RFC 2616, *Hypertext Transfer Protocol—HTTP/1.1*, check the box next to that request method. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if it encounters traffic using that request method.

Content Options

> You can have the router examine the content of HTTP traffic and permit or block traffic, and generate alarms based on what things that you make the router check. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.
>
> Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

Verify Content Type checkbox

> Check if you want the router to verify the content of HTTP packets by matching the response with the request, by enabling an alarm for unknown content types, or by using both of these methods. Use the permit, block, and alarm controls to specify the action the router takes if requests cannot be matched with responses, and when it encounters an unknown content type.

Set Content Length checkbox

Check this box to set a minimum and maximum length for the data in an HTTP packet, and enter the values in the fields provided. Use the permit, block, and alarm controls to specify the action the router takes if the amount of data falls below the minimum length or when it exceeds the maximum length.

Configure Transfer Encoding Checkbox

Check this box to have the router verify how the data in the packet is encoded, and use the permit, block, and alarm controls to specify the action the router takes if it encounters the transfer encodings that you choose.

Chunk checkbox

The Encoding format specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1. The body of the message is transferred in a series of chunks; each chunk contains its own size indicator.

Compress checkbox

The encoding format produced by the UNIX "compress" utility.

Deflate checkbox

The "ZLIB" format defined in RFC 1950, ZLIB Compressed Data Format Specification version 3.3, combined with the "deflate" compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification version 1.3.

gzip checkbox

The encoding format produced by the GNU zip ("gzip") program.

Identity checkbox

Default encoding, which indicates that no encoding has been performed.

Applications/Protocols

This window allows you to create policy settings for applications and protocols that are not found in the other windows. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Applications/Protocols Tree

The Applications/Protocols tree enables you to filter the list on the right according to the type of applications and protocols that you want to view. First choose the branch for the general type that you want to display. The frame on the right displays the available items for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click on the + sign to expand the branch and then select the subcategory that you want to display. If the list on the right is empty, there are no applications or protocols available for that type. To choose an application, you can check the box next to it in the tree, or you can check the box next to it in the list.

Example: If you want to display all Cisco applications, click the **Applications** branch folder, and then click the **Cisco** folder. You will see applications like *clp*, *cisco-net-mgmt*, and *cisco-sys*.

Edit Button

Click this button to edit the settings for the chosen application. Settings that you make override the global settings configured on the router.

Applications Column

The name of the application or protocol, for example *tcp*, *smtp, or ms-sna*. To edit the settings for an item, check the box to the left of the item name, and click **Edit**.

Alerts, Audit, and Timeout Columns

These columns display explicitly-set values for an item. If a setting is not changed for an item, the column is empty. For example, if auditing has been enabled for the ms-sna application, but no changes have been made to the alert or to the timeout settings, the value *on* is displayed in the **Audit** column, but the **Alert** and **Timeout** columns are blank.

Options Column

This column can contain fields if other settings were made for the chosen item.

MAX Data

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login

Causes a user at a nonsecure location to use encryption for authentication.

Reset

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Use this information to help you create or edit a parameter map for inspection purposes, or to set Context-Based Access Control (CBAC) global timeouts and thresholds. CBAC uses timeouts and thresholds to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply to all sessions.

Global Timer values can be specified in seconds, minutes, or hours.

TCP Connection Timeout Value

Amount of time to wait for a TCP connection to be established. The default value is 30 seconds.

TCP FIN Wait Timeout Value

Amount of time that a TCP session will still be managed after the firewall detects a FIN exchange. The default value is 5 seconds.

TCP Idle Timeout Value

Amount of time that a TCP session will still be managed after no activity has been detected. The default value is 3600 seconds.

UDP Idle Timeout Value

Amount of time that a User Datagram Protocol (UDP) session will still be managed after no activity has been detected. The default value is 30 seconds.

DNS Timeout Value

Amount of time that a Domain Name System (DNS) name lookup session will be managed after no activity has been detected. The default value is 5 seconds

SYN Flooding DoS Attack Thresholds

An unusually high number of half-open sessions may indicate that a Denial of Service (DoS) attack is under way. DoS attack thresholds allow the router to start deleting half-open sessions after the total number of them has reached a maximum threshold. By defining thresholds, you can specify when the router should start deleting half-open sessions and when it can stop deleting them.

One-minute session thresholds. These fields let you specify the threshold values for new connection attempts.

Low	Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions.
High	Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions

Maximum incomplete session thresholds. These fields let you specify the threshold values for the total number of existing half-open sessions.

Low	Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions for Cisco IOS releases older than 12.4(11)T. When a Low value is not explicitly set, Cisco IOS will stop deleting new sessions when the number of sessions drops to 400.
	For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a Low value is not explicitly set, Cisco IOS will not stop deleting new connections.
High	Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions for Cisco IOS releases older than 12.4(11)T. When a High value is not explicitly set, Cisco IOS starts deleting sessions when more than 500 new sessions have been established.
	For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a High value is not explicitly set, Cisco IOS will not start deleting new connections.

TCP Maximum Incomplete Sessions per Host:

The router starts deleting half-open sessions for the same host when the total number for that host exceeds this number. The default number of sessions is 50. If you check the **Blocking Time** field and enter a value, the router will continue to block new connections to that host for the number of minutes that you specify.

Enable audit globally

Check if you want to turn on CBAC audit trail messages for all types of traffic.

Enable alert globally

Check if you want to turn on CBAC alert messages for all types of traffic.

Associate Policy with an Interface

In this window, select the interface to which you want to apply the selected policy. Also specify whether the policy is to apply to incoming traffic, to outgoing traffic, or to traffic in both directions.

For example, if the router has FastEthernet 0/0 and FastEthernet 0/1 interfaces, and you want to apply the policy to the FastEthernet 0/1 interface, on traffic flowing in both directions, check the box next to FastEthernet 0/1, and check the boxes in both the Incoming and the Outgoing columns. To have only incoming traffic inspected, only check the box in the Incoming column.

Edit Inspection Rule

Use this window to specify custom inspection rule settings for an application. Settings made here and applied to the router's configuration override the global settings.

Click the **Global Settings** button in the Application Security window to display the global settings for the parameters that you can set in this window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

Alert Field

Choose one of the following values:

- **default**—Use the global setting for alerts.
- **on**—Generate an alert when traffic of this type is encountered.
- **off**—Do not generate an alert when traffic of this type is encountered.

Audit Field

Choose one of the following values:

- **default**—Use the global setting for audit trails.
- **on**—Generate an audit trail when traffic of this type is encountered.
- **off**—Do not generate an audit trail when traffic of this type is encountered.

Timeout Field

Enter the number of seconds that a session for this application should be managed after no activity has been detected. The timeout value that you enter sets the TCP Idle Timeout value if this is a TCP application, or the UDP timeout value if this is a UDP application.

Other Options

Certain applications can have additional options set. Depending on the application, you may see the options described next.

MAX Data field

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure Login Checkbox

Causes a user at a nonsecure location to use encryption for authentication.

Reset Checkbox

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic Checkbox

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Permit, Block, and Alarm Controls

Use the Permit, Block, and Alarm controls to specify what the router is to do when it encounters traffic with the characteristics that you specify. To make a policy setting for an option with these controls, check the box next to it. Then, in the Action column, choose **Permit** to allow traffic related to that option, or choose **Block** to deny traffic. If you want an alarm to be sent to the log when this type of traffic is encountered, check **Send Alarm**. The Send Alarm control is not used in all windows.

Logging must be enabled for Application Security to send alarms to the log. For more information go to this link: Application Security Log.

Site-to-Site VPN

The help topics in this section describe the Site-to-Site VPN configuration screens, and the VPN Design Guide screens.

VPN Design Guide

If you are an administrator setting up a VPN network, the VPN Design Guide helps you to determine which kind of VPN to configure. You provide information about what type of user you are, the type of equipment that the router establishes VPN connections with, the type of traffic that the VPN will carry, and other features that you need to configure. After you provide this information, the VPN Design Guide recommends a VPN type, and allows you to launch the wizard that will enable you to configure that type of VPN.

Create Site to Site VPN

A Virtual Private Network (VPN) lets you protect traffic that travels over lines that your organization may not own or control. VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent.

You can let Cisco Router and Security Device Manager (Cisco SDM) guide you through a simple VPN configuration by clicking the VPN icon. When you use the Wizard in the Create Site-to-Site VPN tab, Cisco SDM provides default values for some configuration parameters in order to simplify the configuration process.

If you want to learn more about VPN technology, there is background information at the link More About VPN.

Create a Site-to-Site VPN

This option allows you to create a VPN network connecting two routers.

Create a Secure GRE Tunnel (GRE-over-IPSec)

This option allows you to configure a generic routing encapsulation protocol (GRE) tunnel between your router and a peer system.

What Do You Want to Do?

If you want to:	Do this:
Configure the router as part of a VPN network connecting two routers.	Select **Create a site-to-site VPN** . Then click **Launch the selected task**.
When you configure a VPN network between two routers, you can control how the remote router is authenticated, how traffic is encrypted, and what traffic is encrypted.	
Configure a GRE tunnel between your router and another router.	Select Create a Secure GRE tunnel (GRE-over-IPSec). Then click **Launch the selected task**.
You may want to configure a GRE tunnel if you need to connect networks that use different LAN protocols, or if you need to send routing protocols over the connection to the remote system.	

If you want to:	Do this:
Find out how to perform other VPN-related tasks that this wizard does not guide you through.	Select a topic from the following list: • How Do I View the IOS Commands I Am Sending to the Router? • How Do I Create a VPN to More Than One Site? • After Configuring a VPN, How Do I Configure the VPN on the Peer Router? • How Do I Edit an Existing VPN Tunnel? • How Do I Confirm That My VPN Is Working? • How Do I Confirm That My VPN Is Working? • How Do I Configure a Backup Peer for My VPN? • How Do I Accommodate Multiple Devices with Different Levels of VPN Support? • How Do I Configure a VPN on an Unsupported Interface? • How Do I Configure a VPN After I Have Configured a Firewall? • How Do I Configure NAT Passthrough for a VPN? • How Do I Configure a DMVPN Manually?

If you want to:	Do this:
Configure an Easy VPN concentrator. Configuration instructions for Easy VPN servers and concentrators are available on www.cisco.com.	The following link provides guidelines to use when configuring a Cisco VPN 3000 series concentrator to operate with an Easy VPN Remote Phase II client, and other information which you might find useful: http://www.cisco.com/en/US/products/sw/ioss wrel/ps5012/products_feature_guide09186a008 00a8565.html The following link connects you to Cisco VPN 3000 series documentation: http://www.cisco.com/en/US/products/hw/vpnd evc/ps2284/products_getting_started_guide_bo ok09186a00800bbe74.html

Site-to-Site VPN Wizard

You can have Cisco SDM use default settings for most of the configuration values, or you can let Cisco SDM guide you in configuring a VPN.

What do you want to do?

If you want to:	Do this:
Quickly configure a site-to-site VPN using Cisco SDM-provided defaults.	Check **Quick setup**, and then click **Next**.
	Cisco SDM will automatically provide a default IKE policy to govern authentication, a default transform set to control the encryption of data and a default IPSec rule that will encrypt all traffic between the router and the remote device.
	Quick setup is best used when both the local router and the remote system are Cisco routers using Cisco SDM.
	Quick setup will configure 3DES encryption if it is supported by the IOS image. Otherwise, it will configure DES encryption. If you need AES or SEAL encryption, click **Step-by-step wizard**.
View the default IKE policy, transform set, and IPSec rule that will be used to configure a One-step VPN.	Click **View Defaults**.
Configure a site-to-site VPN using parameters that you specify.	Check **Step-by-Step wizard**, and then click **Next**.
	You can create a custom configuration for the VPN, and use any of the Cisco SDM defaults that you need.
	Step-by-step wizard allows you to specify stronger encryption than the Quick setup wizard allows.

View Defaults

This window displays the default Internet Key Exchange (IKE) policy, transform set, and IPSec rule that Cisco SDM will use to configure a Quick Setup site-to-site VPN. If you need a different configuration than this window shows, check **Step-by-Step wizard** so that you can define configuration values.

VPN Connection Information

Use this window to identify the IP address or host name of the remote site that will terminate the VPN tunnel that you are configuring, to specify the router interface to use, and to enter the pre-shared key that both routers will use to authenticate each other.

Select the interface for this VPN Connection

Select the interface on this router that connects to the remote site.The router you are configuring is represented as the Local router in the Use Case Scenario diagram.

Peer Identity

Enter the IP address of the remote IP Security (IPSec) peer that will terminate the VPN tunnel you are configuring. The remote IPSec peer might be another router, a VPN concentrator, or any other gateway device that supports IPSec.

Peer(s) with dynamic IP addresses

Select this option if the peers the router connects to use a dynamically-assigned IP addresses.

Peer with static IP address

Select this option if the peer the router connects to uses a fixed IP address.

Enter the IP Address of the remote peer

(Enabled when Peer with static IP address is selected). Enter the IP address of the remote peer.

Authentication

Click this button if the VPN peers use a pre-shared key to authenticate connections from each other. This key must be the same on each side of the VPN connection.

Enter the pre-shared key, and then reenter it for confirmation. Exchange the pre-shared key with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.

Note
- The characters you enter for the pre-shared key are not displayed in the field as you enter them. You may find it helpful to write down the key before you enter it so that you can communicate it to the administrator of the remote system.

- Pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Digital Certificate

Click this button if the VPN peers will use digital certificates for authentication.

Note   The router must have a digital certificate issued by a Certificate Authority to authenticate itself. If you have not configured a digital certificate for the router, go to VPN components, and use the Digital Certificate wizard to enroll for a digital certificate.

Traffic to Encrypt

If you are configuring a Quick Setup site-to-site VPN connection, you need to specify the source and destination subnets in this window.

Source

Choose the interface on the router that will be the source of the traffic on this VPN connection. All traffic coming through this interface whose destination IP address is in the subnet specified in the Destination area will be encrypted.

Details

Click this button to obtain details about the interface you selected. The details window shows any access rules, IPSec policies, Network Address Translation (NAT) rules, or Inspection rules associated with the interface. To examine any of these rules in more detail, go to Additional Tasks/ACL Editor, and examine them in the Rules windows.

Destination

IP address and Subnet Mask. Enter the IP address and subnet mask of the destination for this traffic. For more information about how to enter values in these fields, see IP Addresses and Subnet Masks.

The destination is depicted as the Remote router in the Use Case Scenario diagram in the main VPN wizard window.

IKE Proposals

This window lists all the Internet Key Exchange (IKE) policies that have been configured on the router. If no user-defined policies have been configured, the windows lists the Cisco SDM default IKE policy. IKE policies govern the way that devices in a VPN authenticate themselves.

The local router will use the IKE policies listed in this window to negotiate authentication with the remote router.

The local router and the peer device must both use the same policy. The router that initiates the VPN connection offers the policy with the lowest priority number first. If the remote system rejects that policy, the local router offers the policy with the next lowest number, and continues in this fashion until the remote system accepts. You must coordinate closely with the administrator of the peer system so that you can configure identical policies on both routers.

For Easy VPN connections, IKE policies are only configured on the Easy VPN server. The Easy VPN client sends proposals, and the server responds according to its configured IKE policies.

Priority

This is the order in which the policy will be offered during negotiation.

Encryption

Cisco SDM supports a variety of encryption types, listed in order of security. The more secure an encryption type is, the more processing time it requires.

Note
- Not all routers support all encryption types. Unsupported types will not appear in the screen.

- Not all IOS images support all the encryption types that Cisco SDM supports. Types unsupported by the IOS image will not appear in the screen.

- If hardware encryption is turned on, only those encryption types supported by hardware encryption will appear in the screen.

Cisco SDM supports the following types of encryption:

- DES—Data Encryption Standard. This form of encryption supports 56-bit encryption.

- 3DES—Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.

- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.

- AES-192—AES encryption with a 192-bit key.

- AES-256—AES encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. Cisco SDM supports the following algorithms:

- SHA_1—Secure Hash Algorithm. A hash algorithm used to authenticate packet data.

- MD5—Message Digest 5. A hash algorithm used to authenticate packet data.

D-H Group

The Diffie-Hellman Group—Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. Cisco SDM supports the following groups:

- group1—D-H Group 1. 768-bit D-H Group.
- group2—D-H Group 2. 1024-bit D-H Group. This group provides more security than group 1, but requires more processing time.
- group5—D-H Group 5.1536-bit D-H Group. This group provides more security than group 2, but requires more processing time.

Authentication

The authentication method to be used. The following values are supported:

- PRE_SHARE—Authentication will be performed using pre-shared keys.
- RSA_SIG—Authentication will be performed using digital certificates.

> **Note**   You must choose the authentication type that you specified when you identified the interfaces that the VPN connection is using.

Type

Either Cisco SDM Default or User Defined. If no User Defined policies have been created on the router, this window will show the default IKE policy.

To add or edit an IKE policy:

If you want to add an IKE policy that is not included in this list, click **Add** and create the policy in the window displayed. Edit an existing policy by selecting it and clicking **Edit**. Cisco SDM Default policies are read only, and cannot be edited.

To accept the policy list:

To accept the IKE policy list and continue, click **Next**.

Transform Set

This window lists the Cisco SDM-default transform sets and the additional transform sets that have been configured on this router. These transform sets will be available for use by the VPN or DMVPN. A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms.

You can select only one transform set in this window, but you can associate additional transform sets to the VPN or DMVPN connection using the VPN or DMVPN Edit tabs.

Select Transform Set

Select the transform set that you want to use from this list.

Details of the Selected Transform Set

This area supplies details about the selected transform set. Not all types of encryption, authentication, and compression have to be configured; therefore, some columns may not contain values.

To learn the possible values each column may contain, click **Add or Edit Transform Set**.

Name

The name given to this transform set.

ESP Encryption

The type of Encapsulating Security Protocol (ESP) encryption used. If ESP encryption is not configured for this transform set, this column will be empty.

ESP Authentication

The type of ESP authentication used. If ESP authentication is not configured for this transform set, this column will be empty.

AH Authentication

The type of Authentication Header (AH) authentication used. If AH authentication is not configured for this transform set, this column will be empty.

IP Compression

If IP compression is configured for this transform set, this field contains the value COMP-LZS.

Note   IP compression is not supported on all routers.

Mode

This column contains one of the following:

- Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.

- Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as routers to act as an IPsec proxy for multiple VPN users.

Type

Either User Defined, or Cisco SDM Default.

What Do You Want to Do?

If you want to:	Do this:
Select a transform set for the VPN to use.	Select a transform set, and click **Next**.
Add a transform set to the router's configuration.	Click **Add**, and create the transform set in the Add Transform Set window. Then click **Next** to continue VPN configuration.

If you want to:	Do this:
Edit an existing transform set.	Select a transform set, and click **Edit**. Then, edit the transform set in the Edit Transform Set window. After editing the transform set, click **Next** to continue VPN configuration. Cisco SDM Default transform sets are read only and cannot be edited.
Associate additional transform sets with this VPN.	Select one transform set in this window, and complete the VPN wizard. Then, associate other transform sets to the VPN in the Edit tab.

Traffic to Protect

This window lets you define the traffic that this VPN protects. The VPN can protect traffic between specified subnets, or protect the traffic specified in an IPSec rule that you select.

Protect All Traffic Between the Following Subnets

Use this option to specify a single source subnet (a subnet on the LAN) whose outgoing traffic you want to encrypt, and one destination subnet supported by the peer that you specified in the VPN Connection window.

All traffic flowing between other source and destination pairs will be sent unencrypted.

Source

Enter the address of the subnet whose outgoing traffic you want to protect, and specify the subnet mask. For more information, refer to Available Interface Configurations.

All traffic from this source subnet that has a destination IP address on the destination subnet will be protected.

Destination

Enter the address of the destination subnet, and specify the mask for that subnet. You can select a subnet mask from the list, or type in a custom mask. The subnet number and mask must be entered in dotted decimal format, as shown in the previous examples.

All traffic going to the hosts in this subnet will be protected.

Create/Select an access-list for IPSec traffic

Use this option if you need to specify multiple sources and destinations, and/or specific types of traffic to encrypt. An IPSec rule can consist of multiple entries, each specifying different traffic types and different sources and destinations.

Click the button next to the field, and specify an existing IPSec rule that defines the traffic you want to encrypt, or create an IPSec rule to use for this VPN. If you know the number of the IPSec rule, enter it in the box to the right. If you do not know the number of the rule, click the **...** button and browse for the rule. When you select the rule, the number will appear in the box.

> **Note**   Because they can specify traffic type, and both source and destination, IPSec rules are extended rules. If you enter the number or name of a standard rule, a Warning message is displayed indicating that you have entered the name or number of a standard rule.

Any packets that do not match the criteria in the IPSec rule are sent with no encryption.

Summary of the Configuration

This window shows you the VPN or DMVPN configuration that you created. You can review the configuration in this window and use the back button to make changes if you want.

Spoke Configuration

If you have configured a DMVPN hub, you can have Cisco SDM generate a procedure that will assist you or other administrators in configuring DMVPN spokes. The procedure explains which options to select in the wizard, and what information to enter in spoke configuration windows. You can save this information to a text file that you or another administrator can use.

Test the connectivity after configuring

Click to test the VPN connection you have just configured. The results of the test will be shown in another window.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish.** Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco SDM Preferences window, the Deliver window will appear . In this window, you can view the CLI commands you that are delivering to the router.

Spoke Configuration

This window contains information that you can use to give a spoke router a configuration that will be compatible with the DMVPN hub that you configured. It lists the windows you need to complete, giving you data that you need to enter in the window so that the spoke will be able to communicate with the hub.

It provides the following data that you need to input into the spoke configuration:

- The hub's public IP address. This is the IP address of the hub interface that supports the mGRE tunnel.

- The IP address of the hub's mGRE tunnel.

- The subnet mask that all tunnel interfaces in the DMVPN must use.

- The advanced tunnel configuration information.

- The routing protocol to use, and any information associated with the protocol, such as Autonomous System number (for EIGRP), and OSPF Process ID.

- The hash, encryption, DH group, and Authentication Type of the IKE policies that the hub uses, so that compatible IKE policies can be configured on the spoke.

- The ESP and Mode information of the transform sets that the hub uses. If similar transform sets have not been configured on the spoke, they can be configured using this information.

Secure GRE Tunnel (GRE-over-IPSec)

Generic routing encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

This wizard enables you to create a GRE tunnel with IPSec encryption. When you create a GRE tunnel configuration, you also create an IPSec rule that describes the endpoints of the tunnel.

GRE Tunnel Information

General GRE tunnel information is provided in this screen.

Tunnel Source

Select the interface name or the IP address of the interface that the tunnel will use. The IP address of the interface must be reachable from the other end of the tunnel; therefore it must a a public, routable IP address. An error will be generated if you enter an IP address that is not associated with any configured interface.

Note   Cisco SDM lists interfaces with static IP addresses and interfaces configured as unnumbered in the Interface list. Loopback interfaces are not included in the list.

Details

Click to obtain details about the interface that you selected. The details window shows any access rules, IPSec policies, NAT rules, or Inspection rules associated with the interface. If a NAT rule has been applied to this interface that causes the address to be unroutable, the tunnel will not operate properly. To examine any of these rules in more detail, go to Additional Tasks/ACL Editor and examine the in the Rules window.

Tunnel Destination

Enter the IP address of the interface on the remote router at the other end of the tunnel. This is the source interface from the point of view of the other end of the tunnel.

Make sure that this address is reachable by using the **ping** command. The **ping** command is available from the Tools menu. If the destination address cannot be reached, the tunnel will not be created properly.

IP Address of the GRE tunnel

Enter the IP address of the tunnel. The IP addresses of both ends of the tunnel must be in the same subnet. The tunnel is given a separate IP address so that it can be a private address, if necessary.

IP Address

Enter the IP address of the tunnel in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask for the tunnel address in dotted decimal format.

VPN Authentication Information

VPN peers use a pre-shared key to authenticate connections from each other. This key must be the same on each side of the VPN connection.

Pre-Shared Key

Click this button if the VPN peers use a pre-shared key for authentication and then enter the pre-shared key, and then reenter it for confirmation. Exchange the pre-shared key with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key.

> **Note**
> - The characters that you enter for the pre-shared key are not displayed in the field as you enter them. You may find it helpful to write down the key before you enter it so that you can communicate it to the administrator of the remote system.
>
> - Pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Digital Certificate

Click this button if the VPN peers will use digital certificates for authentication.

The router must have a digital certificate issued by a Certificate Authority to authenticate itself. If you have not configured a digital certificate for the router, go to VPN components, and use the Digital Certificate wizard to enroll for a digital certificate.

> **Note**
> If you are authenticating using digital certificates, the VPN tunnel might not be created if the CA server contacted during IKE negotiation is not configured to respond to Certificate Revocation List (CRL) requests. To correct this problem, go to the Digital Certificates page, select the configured trustpoint, and select None for Revocation.

Backup GRE Tunnel Information

You can configure a backup GRE-over-IPSec tunnel that the router can use when the primary tunnel fails. This tunnel will use the same interface that you configured for the primary tunnel, but it must be configured with the backup VPN router as the peer. If routing is configured for the primary GRE-over-IPSec tunnel, the keepalive packets that the routing protocol sends are used to verify that the tunnel is still active. If the router stops receiving keepalive packets on the primary tunnel, then traffic is sent through the backup tunnel.

Create a backup secure GRE tunnel for resilience

Check this box if you want to create a backup tunnel.

IP address of the backup GRE tunnel's destination

Enter the IP address of the interface on the remote router at the other end of the tunnel. (This is the source interface from the point of view of the other end of the tunnel.)

Make sure that this address is reachable by using the **ping** command. The **ping** command is available from the Tools menu. If the destination address specified in the Ping dialog cannot be reached, the tunnel will not be created properly.

Tunnel IP address

Enter the IP address of the tunnel. The IP addresses of both ends of the tunnel must be in the same subnet. The tunnel is given a separate IP address so that it can be a private address, if necessary.

IP Address

Enter the IP address of the tunnel in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask for the tunnel address in dotted decimal format.

Routing Information

This window enables you to configure routing for the tunneled traffic. Information that you add in this window appears in the Routing window. Changes that you make in the Routing window may affect routing of VPN traffic. Configuring routing enables you to specify the networks that will participate in the GRE-over-IPSec VPN. Additionally, if you configure a backup GRE-over-IPSec tunnel, the keepalive packets sent by routing protocols allow the router to determine whether the primary tunnel has failed.

Select a dynamic routing protocol if this router is being used in a large VPN deployment with a large number of networks in the GRE over IPSec VPN. Select static routing if a small number of networks will participate in the VPN.

EIGRP

Check this box to use the Enhanced Interior Gateway Routing Protocol (EIGRP) protocol to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

OSPF

Check this box to use the Open Shortest Path First protocol (OSPF) to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

RIP

Check this box to use the Routing Information Protocol(RIP) to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

$\diagdown$

Note   This option is not available when you configure a backup GRE-over-IPSec tunnel.

Static Routing

Static routing can be used in smaller VPN deployments in which only a few private networks participate in the GRE-over-IPSec VPN. You can configure a static route for each remote network so that traffic destned for the remote networks will pass through the appropriate tunnels.

Static Routing Information

You can configure a static route for each remote network so that traffic destined for the remote networks will pass through the appropriate tunnels. Configure the first static route in the Static Routing Information window. If you need to configure additional static routes, you can do so in the Routing window.

Check this box if you want to specify a static route for the tunnel, and select one of the following:

- **Tunnel all traffic**—All traffic will be routed through the tunnel interface and encrypted. Cisco SDM creates a default static route entry with the tunnel interface as the next hop.

  If a default route already exists, Cisco SDM modifies that route to use the tunnel interface as the next hop, replacing the interface that was originally there, and creates a new static entry to the tunnel destination network that specifies the interface in the original default route as the next hop.

  The following example assumes the network at the other end of the tunnel is 200.1.0.0, as specified in the destination network fields:

  ```
  ! Original entry

  ip route 0.0.0.0  0.0.0.0 FE0

  ! Entry changed by SDM

  ip route 0.0.0.0  0.0.0.0 Tunnel0

  ! Entry added by SDM

  ip route 200.1.0.0  255.255.0.0 FE0
  ```

  If no default route exists, Cisco SDM simply creates one, using the tunnel interface as the next hop. For example:

  ```
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ```

- **Do split tunneling**—Split tunneling allows traffic that is destined for the network specified in the IP Address and Network Mask fields to be encrypted and routed through the tunnel interface. All other traffic will not be encrypted. When this option is selected, Cisco SDM creates a static route to the network, using the IP address and network mask.

  The following example assumes that the network address 10.2.0.0/255.255.0.0 was entered in the destination address fields:

  The following example assumes that the network address 10.2.0.0/255.255.0.0 was entered in the destination address fields:

  ```
  ip route 10.2.0.0 255.255.0.0 Tunnel0
  ```

When split tunneling is selected, the IP Address and Subnet Mask fields will appear, requiring you to enter the IP Address and Subnet Mask of the destination peer. You must ensure that the destination IP address entered in the Tunnel Destination field of the GRE Tunnel Information window is reachable. If it is not reachable, no tunnel will be established.

IP Address

Enabled with split tunneling. Enter the IP address of the network at the other end of the tunnel. Cisco SDM will create a static route entry for the packets with a destination address in that network. This field is disabled when **Tunnel all traffic** is selected.

You must ensure that the IP address entered in this field is reachable before you configure this option. If it is not reachable, no tunnel will be established.

Network Mask

Enabled with split tunneling. Enter the network mask used on the network at the other end of the tunnel. This field is disabled when **Tunnel all traffic** is selected.

Select Routing Protocol

Use this window to specify how other networks behind your router are advertised to the other routers in the network. Select one of the following:

- EIGRP—Extended Interior Gateway Routing Protocol.
- OSPF—Open Shortest Path First.
- RIP—Routing Internet Protocol.
- Static Routing. This option is enabled when you are configuring a GRE over IPSec tunnel.

Note RIP is not supported for DMVPN Hub and spoke topology but is available for DMVPN Full Mesh topology.

Summary of Configuration

This screen summarizes the GRE configuration that you have completed. You can review the information in this screen and click the back button to return to any screen in which you want to make changes. If you want to save the configuration, click **Finish**.

GRE tunnel configuration creates an IPSec rule that specifies which hosts the GRE traffic will be allowed to flow between. This IPSec rule is displayed in the summary.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco SDM saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco SDM Preferences window, the Deliver window will appear . In this window, you can view the CLI commands you that are delivering to the router.

Edit Site-to-Site VPN

Virtual Private Networks (VPNs) let you protect data between your router and a remote system by encrypting traffic so that it cannot be read by others who are using the same public network. In effect, it gives you the protection of a private network over public lines that may be used by other organizations.

Use this window to create and manage VPN connections to remote systems. You can create, edit, and delete VPN connections, and reset existing connections. You can also use this window to configure your router as an Easy VPN client with connections to one or more Easy VPN servers or concentrators.

Click the link for the part of the window for which you want help:

Site-to-Site VPN Connections

VPN connections, sometimes referred to as *tunnels*, are created and managed from the VPN Connections box. A VPN connection links a router interface to one or more peers specified by a crypto map defined in an IP Security (IPSec) policy.You can view, add, edit, and delete the VPN connections in this list.

Status column

The status of the connection, which is indicated by the following icons:

The connection is up.

The connection is down.

The connection is being established.

Interface

The router interface that is connected to the remote peers in this VPN connection. An interface can be associated with only one IPSec policy. The same interface will appear on multiple lines if there is more than one crypto map defined for the IPSec policy used in this connection.

Description

A short description of this connection.

IPSec Policy

The name of the IPSec policy used in this VPN connection. The IPSec policy specifies how data is encrypted, which data will be encrypted, and where data will be sent. For more information, click More about VPN Connections and IPSec Policies.

Sequence Number

The sequence number for this connection. Because an IPSec policy may be used in more than one connection, the combination of the sequence number and IPSec policy name uniquely identifies this VPN connection. The sequence number does not prioritize the VPN connection; the router will attempt to establish all configured VPN connections regardless of sequence number.

Peers

The IP addresses or host names of the devices at the other end of the VPN connection. When a connection contains multiple peers, their IP addresses or host names are separated by commas. Multiple peers might be configured to provide alternative routing paths for the VPN connection.

Transform Set

This shows the name of the transform set used by this VPN connection. Multiple transform set names are separated by commas. A transform set specifies the algorithms that will be used to encrypt data, ensure data integrity, and provide data compression. Both peers must use the same transform set, and they negotiate to determine which set they will use. Multiple transform sets may be defined to ensure that the router can offer a transform set that the negotiating peer will agree to use. The transform sets is a component of the IPSec policy.

IPSec Rule

The rule that determines which traffic should be encrypted on this connection. The IPSec rule is a component of the IPSec Policy.

Type

One of the following:

- Static—This is a static site-to-site VPN tunnel. The VPN tunnel uses static crypto maps.

- Dynamic—This is a dynamic site-to-site VPN tunnel. The VPN tunnel uses dynamic crypto maps.

Add Button

Click to add a VPN connection

Delete Button

Click to delete a selected VPN connection

Test Tunnel.. Button

Click to test a selected VPN tunnel.The results of the test will be shown in another window.

Clear Connection Button

Click to reset an established connection to a remote peer. This button is disabled if you have selected a dynamic site-to-site VPN tunnel.

Generate Mirror..Button

Click to create a text file that captures the VPN configuration of the local router so that a remote router can be given a VPN configuration that enables it to establish a VPN connection to the local router. This button is disabled if you have selected a dynamic site-to-site VPN tunnel.

Note Any previously configured VPN connections detected by Cisco SDM that do not use ISAKMP crypto maps will appear as read-only entries in the VPN connection table and cannot be edited.

Add new connection

Use this window to add a new VPN connection between the local router and a remote system, referred to as a *peer*. You create the VPN connection by associating an IPSec policy with an interface.

To create a VPN connection:

Step 1 Select the interface you want to use for the VPN from the Select Interface list. Only interfaces that are not used in other VPN connections are shown in this list.

Step 2 Select a policy from the Choose IPSec Policy list. Click **OK** to return to the VPN Connections window.

Add Additional Crypto Maps

Use this window to add a new crypto map to an existing IPSec policy. This window shows the interface associated with the VPN connection that you selected in the VPN Connections window, the IPSec policy associated with it, and the crypto maps that the policy already contains.

The crypto map specifies a sequence number, the peer device at the other end of the connection, the set of transforms that encrypt the traffic, and the IPSec rule that determines which traffic is encrypted.

Note   Adding a crypto map to an existing IPSec policy is the only way to add a VPN tunnel to an interface that is already being used in an existing VPN connection.

Interface

This is the interface used in this VPN connection.

IPSec Policy

This is the name of the IPSec policy controlling the VPN connection. The crypto maps making up the IPSec policy are shown in the list below this field. For more information, click More about VPN Connections and IPSec Policies.

What Do You Want to Do?

If you want to:	Do this:
Configure the crypto map yourself.	Click **Add New Crypto Map** and use the Add Crypto Map window to create the new crypto map. Click **OK** when you are finished. Then click **OK** in this window.
Have Cisco Router and Security Device Manager (Cisco SDM) help you add a new crypto map to this connection.	Check the **Use Add Wizard** box, and click **OK**. Cisco SDM will guide you in creating a new crypto map, and will associate it with the IPSec policy.

Crypto Map Wizard: Welcome

This wizard will guide you through the creation of a crypto map. A crypto map specifies the peer devices at the other end of the VPN connection, defines how traffic will be encrypted, and identifies which traffic will be encrypted.

Click **Next** to begin creating a crypto map.

Crypto Map Wizard: Summary of the configuration

The Cryptomap wizard summary page displays the data you entered in the wizard windows. You can review it, click Back to return to a screen to make changes, and then return to the Summary window and click **Finish** to deliver the cryptomap configuration to the router.

Delete Connection

Use this window to delete a VPN tunnel, or simply to disassociate it from an interface but preserve the definition for future use.

Delete the crypto map with sequence number *n* from IPSec policy *policy name*

Click this button, and then click **OK** to remove the VPN tunnel definition. The associations created between the interface, IPSec policy, and peer devices will be lost when you do this. If more than one interface has been associated with this tunnel definition, those associations are deleted as well.

Delete the dynamic crypto map with sequence number *n* from the dynamic crypto map set *set name*

This button is shown if you selected a dynamic site-to-site VPN tunnel. Click this button, and then click **OK** to remove the VPN tunnel definition. The associations created between the interface, IPSec policy, and peer devices will be lost when you do this. If more than one interface has been associated with this tunnel definition, those associations are deleted as well.

Disassociate the IPSec policy *policy name* from the interface *interface name*, and keep the IPSec policy for possible future reuse

Click this button, and then click **OK** to retain the tunnel definition but remove its association with the interface. You will be able to associate this definition with another router interface if you wish.

Ping

You can ping a peer device in this window. You can select both the source and destination of the ping operation. You may want to ping a remote peer after you reset a VPN tunnel.

Source

Select or enter the IP address where you want the ping to originate. If the address you want to use is not in the list, you can enter a different one in the field. The ping can originate from any interface on the router. By default, the **ping** command originates from the outside interface with the connection to the remote device.

Destination

Select the IP address that you want to ping. If the address you want to use is not in the list, you can enter a different one in the field.

To ping a remote peer:

Specify the source and destination, and click **Ping**. You can read the output of the **ping** command to determine whether the ping was successful.

To clear the output of the ping command:

Click **Clear**.

Generate Mirror...

This window shows you the IPSec policy used for the VPN tunnel to the selected peer, and allows you to save the policy in a text file that you can use when configuring the VPN connection on the peer device.

Peer Device

Select the IP address or host name of the peer device to see the IPSec policy configured for the tunnel to that device. The policy appears in the box under the peer IP address.

To create a text file of the IPSec policy:

Click **Save**, and specify a name and location for the text file. You can give this text file to the administrator of the peer device so that he or she can create a policy that mirrors the one you created on the router. Click **After Configuring a VPN, How Do I Configure the VPN on the Peer Router?** to learn how to use the text file to create a mirror policy.

⚠

Caution   The text file that you generate must not be copied into the configuration file of the remote system, but must be used only to show what has been configured on the local router so that the remote device can be configured in a way that is compatible. Identical names for IPSec policies, IKE policies, and transform sets may be used on the remote router, but the policies and transform sets may be different. If the text file is simply copied into the remote configuration file, configuration errors are likely to result.

Cisco SDM Warning: NAT Rules with ACL

This window appears when you are configuring a VPN using interfaces with associated NAT rules that use Access rules. This type of NAT rule can change IP addresses in packets before the packets leave or enter the LAN, and a NAT rule will prevent VPN connections from functioning properly if it changes source IP addresses so that they don't match the IPSec rule configured for the VPN. To prevent this from happening, Cisco SDM can convert these to NAT rules that use route maps. Route maps specify subnets that should not be translated.

The window shows the NAT rules that have to be changed to ensure the VPN connection functions properly.

Original Address

The IP address that NAT will translate.

Translated Address

The IP address that NAT will substitute for the original address.

Rule Type

The type of NAT rule, either Static or Dynamic.

To make the listed NAT rules use route maps:

Click **OK**.

How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Create a VPN to More Than One Site?

You can use Cisco SDM to create multiple VPN tunnels on one interface on your router. Each VPN tunnel will connect the selected interface on your router to a different subnet at the destination router. You can configure multiple VPN tunnels to connect to the same interface but to different subnets on the destination router, or you can configure multiple VPN tunnels that will connect to different interfaces on the destination router.

First, you must create the initial VPN tunnel. The steps below describe how to create the initial VPN tunnel. If you have already created your first VPN tunnel and need to add an additional tunnel to the same interface, skip the first procedure and perform the steps in the next procedure in this help topic.

Create the initial VPN tunnel:

Step 1	From the left frame, select **VPN**.
Step 2	Select **Create a Site-to-Site VPN** .
Step 3	Click **Launch the Selected Task**.
	The VPN Wizard starts.
Step 4	Click **Quick Setup**.
Step 5	Click **Next>**.

Step 6   From the Select the Router Interface for this VPN Connection field, choose the interface on the source router on which to create the VPN tunnel. This is the interface connected to the Internet on the Local system in the Use Case Scenario diagram.

Step 7   In the Peer Identity field, enter the IP address of the destination router interface.

Step 8   In the Authentication fields, enter and reenter the pre-shared key that the two VPN peers will use.

Step 9   In the Source field, select the interface that connects to the subnet whose IP traffic you want to protect. This is the Local router in the Use Case Scenario diagram, and is usually an interface connected to the LAN.

Step 10   In the Destination fields, enter the IP address and subnet mask of the destination router.

Step 11   Click **Next>**.

Step 12   Click **Finish**.

Create an Additional Tunnel from the Same Source Interface

After you have created the initial VPN tunnel, follow these steps to create an additional tunnel from the same source interface to a different destination interface or destination subnet:

Step 1   From the left frame, select **VPN**.

Step 2   Select **Create a Site-to-Site VPN**.

Step 3   Click **Launch the Selected Task**.

The VPN Wizard starts.

Step 4   Click **Quick Setup**.

Step 5   Click **Next>**.

Step 6   From the Select the Router Interface for this VPN Connection field, choose the same interface that you used to create the initial VPN connection.

Step 7   In the Peer Identity field, enter the IP address of the destination router interface. You can enter the same IP address that you entered when you created the initial VPN connection. This indicates that this second VPN connection should use the

same interface on the destination router as the initial VPN connection. If you do not want both VPN connections to connect to the same destination interface, enter the IP address of a different interface on the destination router.

Step 8   In the Authentication fields, enter and reenter the pre-shared key that the two VPN peers will use.

Step 9   In the Source field, select the same interface used to create the initial VPN connection.

Step 10   In the Destination fields, you have the following options:

- If, in the Peer Identity field, you entered the IP address of a different interface on the destination router and want to protect the IP traffic coming from a specific subnet, enter the IP address and subnet mask of that subnet in the appropriate fields.

- If you entered the same IP address in the Peer Identity field as you used for the initial VPN connection, indicating that this VPN tunnel will use the same router interface as the initial VPN tunnel, then enter the IP address and subnet mask of the new subnet that you want to protect in the appropriate fields.

Step 11   Click **Next>**.

Step 12   Click **Finish**.

After Configuring a VPN, How Do I Configure the VPN on the Peer Router?

Cisco SDM generates VPN configurations on your router. Cisco SDM includes a function that will generate a text file of the configuration that can be used as a template to create a VPN configuration for the peer router to which your VPN tunnel connects. This text file can only be used as a template that shows you which commands need to be configured. It cannot be used without editing because it contains information that is only correct for the local router you configured.

To generate a template configuration for the peer VPN router:

Step 1   From the left frame, select **VPN**.

Step 2   Select **Site-to-Site VPN**. in the VPN tree, and then click the Edit tab.

Step 3   Select the VPN connection that you want to use as a template, and click **Generate Mirror**.

Cisco SDM displays the Generate Mirror screen.

Step 4   From the Peer Device field, select the IP address of the peer device for which you want to generate a suggested configuration.

The suggested configuration for the peer device appears on the Generate Mirror screen.

Step 5   Click **Save** to display the Windows Save File dialog box, and save the file.

⚠️

Caution   Do not apply the mirror configuration to the peer device without editing! This configuration is a template that requires additional manual configuration. Use it only as a starting point to build the configuration for the VPN peer.

Step 6   After saving the file, use a text editor to make any needed changes to the template configuration. These are some commands that may need editing:

- The peer IP address command(s)
- The transform policy command(s)
- The crypto map IP address command(s)
- The ACL command(s)
- The interface ip address command(s)

Step 7   After you have finished editing the peer configuration file, deliver it to the peer router using a TFTP server.

How Do I Edit an Existing VPN Tunnel?

To edit an existing VPN tunnel:

Step 1   From the left frame, select **VPN**.

Step 2   Select **Site-to-Site VPN**. in the VPN tree, and then click the Edit tab.

Step 3   Click the connection that you want to edit.

Step 4   Click **Add.**

Step 5   Select **Static crypto maps to <policy name>**

Step 6   In the Add static crypto maps window, you can add more crypto maps to the VPN connection.

Step 7   If you need to modify any of the components of the connection, such as the IPSec policy or the existing crypto map, note the names of those components in the VPN window, and go to the appropriate windows under VPN Components to make changes.

How Do I Confirm That My VPN Is Working?

You can verify that your VPN connection is working by using the Monitor mode in Cisco SDM. If your VPN connection is working, Monitor mode will display the VPN connection by identifying the source and destination peer IP addresses. Depending on whether your VPN connection is an IPSec tunnel or an Internet Key Exchange (IKE) security association (SA), Monitor mode will display the number of packets transferred across the connection, or show the current state of the connection. To display the current information about a VPN connection:

Step 1   From the toolbar, select **Monitor Mode**.

Step 2   From the left frame, select **VPN Status**.

Step 3   From the Select A Category field, select whether to view information for IPSec tunnels or IKE SAs.

Each configured VPN connection will appear as a row on the screen.

If you are viewing IPSec tunnel information, you can verify the following information to determine that your VPN connection is working:

- The local and remote peer IP addresses are correct, indicating that the VPN connection is between the correct sites and router interfaces.

- The tunnel status is "up." If the tunnel status is "down" or "administratively down," then the VPN connection is not active.

- The number of encapsulation and decapsulation packets is not zero, indicating that data has been transferred over the connection and that the sent and received errors are not too high.

If you are viewing IKE SA information, you can verify that your VPN connection is working by verifying that the source and destination IP addresses are correct, and that the state is "QM_IDLE," indicating that the connection has been authenticated and that data transfer can take place.

How Do I Configure a Backup Peer for My VPN?

To configure multiple VPN peers inside a single crypto map:

Step 1   From the left frame, select **VPN**.

Step 2   From the VPN tree, select **VPN Components**, and then **IPSec Policies**.

Step 3   In the IPSec Policies table, click the IPSec policy to which you want to add another VPN peer.

Step 4   Click **Edit**.

The Edit IPSec Policy dialog box appears.

Step 5   Click **Add**.

Step 6   The Add Crypto Map dialog box appears, letting you set the values for the new crypto map. Set the values for the new crypto map, using all four tabs in the dialog box. The Peer Information tab contains the Specify Peers field, which lets you enter the IP address of the peer you want to add.

Step 7   When you have finished, click **OK**.

The crypto map with the new peer IP address appears in the "Crypto Maps in this IPSec Policy" table.

Step 8   To add additional peers, repeat Step 4 through Step 8.

How Do I Accommodate Multiple Devices with Different Levels of VPN Support?

To add multiple transform sets to a single crypto map:

Step 1   From the left frame, select **VPN**.

Step 2   From the VPN tree, select **VPN Components**, and then **IPSec Policies**.

Step 3   In the IPSec Policies table, click the IPSec policy that contains the crypto map to which you want to add another transform set.

Step 4   Click **Edit**.

The Edit IPSec Policy dialog box appears.

Step 5   In the "Crypto Maps in this IPSec Policy" table, click the crypto map to which you want to add another transform set.

Step 6   Click **Edit**.

The Edit Crypt Map dialog box appears.

Step 7   Click the **Transform Sets** tab.

Step 8   In the Available Transform Sets field, click a transform set that you want to add to the crypto map.

Step 9   Click **>>** to add the selected transform set to the crypto map.

Step 10   If you want to add additional transform sets to this crypto map, repeat Step 9 and Step 10 until you have added all the transform sets you want.

Click **OK**.

How Do I Configure a VPN on an Unsupported Interface?

Cisco SDM can configure a VPN over an interface type unsupported by Cisco SDM. Before you can configure the VPN connection, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is "Up."

After you have configured the unsupported interface using the CLI, you can use Cisco SDM to configure your VPN connection. The unsupported interface will appear in the fields that require you to choose an interface for the VPN connection.

How Do I Configure a VPN After I Have Configured a Firewall?

In order for a VPN to function with a firewall in place, the firewall must be configured to permit traffic between the local and remote peer IP addresses. Cisco SDM creates this configuration by default when you configure a VPN configuration after you have already configured a firewall.

How Do I Configure NAT Passthrough for a VPN?

If you are using NAT to translate addresses from networks outside your own and if you are also connecting to a specific site outside your network via a VPN, you must configure NAT passthrough for your VPN connection, so that network address translation does not take place on the VPN traffic. If you have already configured NAT on your router and are now configuring a new VPN connection using Cisco SDM, you will receive a warning message informing you that Cisco SDM will configure NAT so that it does not translate VPN traffic. You must accept the message so that Cisco SDM will create the necessary ACLs to protect your VPN traffic from translation.

If you are configuring NAT using Cisco SDM and you have already configured a VPN connection, perform the following procedure to create ACLs.

Step 1 From the left frame, select **Additional Tasks/ACL Editor**.

Step 2 In the Rules tree, choose **Access Rules**.

Step 3 Click **Add**.

The Add a Rule dialog box appears.

Step 4 In the Name/Number field, enter a unique name or number for the new rule.

Step 5 From the Type field, choose **Extended Rule**.

Step 6 In the Description field, enter a short description of the new rule.

Step 7 Click **Add**.

The Add a Standard Rule Entry dialog box appears.

Step 8 In the Action field, choose **Permit**.

Step 9 In the Source Host/Network group, from the Type field, select **A Network**.

Step 10   In the IP Address and Wildcard Mask fields, enter the IP address and subnet mask of the VPN source peer.

Step 11   In the Destination Host/Network group, from the Type field, select **A Network**.

Step 12   In the IP Address and Wildcard Mask fields, enter the IP address and subnet mask of the VPN destination peer.

Step 13   In the Description field, enter a short description of the network or host.

Step 14   Click **OK**.

The new rule now appears in the Access Rules table.

How Do I...

C H A P T E R **12**

Easy VPN Remote

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After the Cisco Easy VPN server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series router or a Cisco 2800 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime.

- Establishing tunnels according to the parameters that were set.

- Automatically creating the NAT or Port Address Translation (PAT) and associated access lists that are needed, if any.

- Authenticating users, that is, ensuring that users are who they say they are by way of usernames, group names, and passwords.
- Managing security keys for encryption and decryption.

Cisco SDM provides a wizard that guides you through Easy VPN Remote configuration. You can also edit an existing configuration using Easy VPN Remote edit screens.

This chapter contains the following sections:

- Creating an Easy VPN Remote Connection
- Administering Easy VPN Remote Connections
- Other Procedures

Creating an Easy VPN Remote Connection

Create an Easy VPN Remote connection by using the Easy VPN Remote wizard. Complete these steps:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit** > **Preferences** > **Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   On the Cisco SDM toolbar, click **Configure**.

Step 3   On the Cisco SDM category bar, click **VPN**.

Step 4   In the VPN tree, choose **Easy VPN Remote**.

Step 5   In the Create Easy VPN Remote tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco SDM either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 6   Click **Launch Easy VPN Remote Wizard** to begin configuring the connection.

Step 7   Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 8   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 9   If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 10   To send the configuration to the router, click **Finish**.

Step 11   If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **OK** to send the configuration to the router, or click **Cancel** to discard it. If you did not make this setting, clicking Finish sends the configuration to the router.

The section Create Easy VPN Remote Reference contains detailed information about the screens you use.

Create Easy VPN Remote Reference

The following topics describe the Create Easy VPN Remote screens:

- Create Easy VPN Remote
- Configure an Easy VPN Remote Client
- Easy VPN Remote Wizard: Network Information
- Easy VPN Remote Wizard: Identical Address Configuration
- Easy VPN Remote Wizard: Interfaces and Connection Settings
- Easy VPN Remote Wizard: Server Information
- Easy VPN Remote Wizard: Authentication
- Easy VPN Remote Wizard: Summary of Configuration

Create Easy VPN Remote

Cisco SDM allows you to configure your router as a client to an Easy VPN server or concentrator. Your router must be running a Cisco IOS software image that supports Easy VPN Phase II. The Create Easy VPN Remote tab enables you to launch the Easy VPN Remote wizard.

To be able to complete the configuration, you must have the following information ready.

- Easy VPN server's IP address or hostname

- IPSec group name

- Key

- Whether or not there are devices on the local network with IP addresses that conflict with addresses used in networks that the Easy VPN Remote client will connect to.

Field Reference

Table 12-1 describes the fields in this screen.

Table 12-1　　*Create Easy VPN Remote Tab Felds*

Element	Description
Use Case Scenario	This area displays a network diagram that depicts the type of connection that the wizard enables you to configure.
Recommended Tasks	This area describes recommended tasks to complete before beginning the Easy VPN Remote configuration. Click the link for a particular task to complete it.
	If the Cisco IOS image on the router is version 12.4(9)T or later, Cisco SDM displays the recommended task Enable DNS if DNS is not enabled on the router so that a Split DNS configuration, if pushed by the server, will work.
Launch Easy VPN Remote Wizard	Click **Launch Easy VPN Remote Wizard** to start the wizard.

Configure an Easy VPN Remote Client

This wizard guides you through the configuration of an Easy VPN Remote Phase II Client.

> **Note**   If the router is not running a Cisco IOS image that supports Easy VPN Remote Phase II or later, you will not be able to configure an Easy VPN client.

Easy VPN Remote Wizard: Network Information

Indicate whether or not there are IP addresses in the local network that overlap with IP addresses in networks that the router connects to through the Easy VPN server in this screen. Also, indicate if there are devices on the local network that must be reached from those networks.

> **Note**   This screen is displayed when the Cisco IOS image on the router is version 12.4(11)T or later.

Field Reference

Table 12-2 describes the fields in th is screen.

Table 12-2   Network Information Fields

Element	Description
Client IP Addressing	
Does your client location have an addressing scheme that might overlap with other client locations?	Yes—Click **Yes** if devices on your local network use IP addresses that are also used by devices in other networks that the router will connect to through the Easy VPN Server. For example, printers on the local network may use IP addresses that are used by devices in the peer network. If you click Yes, Cisco SDM displays the Device Reachability fields.
	No—Click **No** if devices on the local network do not use IP addresses that are also used in networks that the router connects to through the Easy VPN server.

Table 12-2   Network Information Fields (continued)

Element	Description
Device Reachability	
Do you have devices at your client location that must be reached from the server-side networks or other client locations?	Yes—Click **Yes** if there are devices on the local network, such as printers, that must be reached from networks that the router connects to through the Easy VPN server.
	No—Click **No** if there are no devices that must be reached from networks that the router connects to through the Easy VPN server.

Easy VPN Remote Wizard: Identical Address Configuration

Enter the local and global IP addresses of the devices that must be reached from networks that the router connects to through the Easy VPN server in this screen.

Field Reference

Table 12-3 describes the fields in th is screen.

Table 12-3   Identical Address Configuration Fields

Element	Description
Accessible Devices	
Device Local IP	The local IP address of a device that is identified as a device that must be reached by other networks.
Device Global IP	The global IP address given to a device that is identified as a device that must be reached by other networks. Because the global IP address for each device must be routable from the Easy VPN server, you must obtain these addresses from the Easy VPN server administrator. Each IP address must be on the same subnet, and one address must be reserved for use by non accessible devices on the local network.
Add	To add the local IP address and global IP address of a device, click **Add**.
Edit	To change the IP address information for a device, choose an entry and click **Edit**.
Delete	To remove an entry for an accessible device, choose the entry and click **Delete**.

Table 12-3   Identical Address Configuration Fields (continued)

Element	Description
Non Accessible Devices	
IP Address	Enter the IP address that you reserved for non accessible devices in this field. This IP address must be in the same subnet as the device global IP addresses. Cisco SDM creates a NAT rule to translate IP addresses of devices that do not need to be reached from other networks to this IP address, and assigns this IP address to a new loopback interface.
Subnet Mask	Enter the subnet mask in decimal format; for example, 255.255.255.0. Or, choose the number of subnet bits; for example, 24. Entering values in one field updates the other. For example, if you enter 255.255.255.0, the subnet bits field is automatically updated to display 24.

Warning Messages

Cisco SDM displays a warning message when you click **Next** if it detects any of the following problems:

- There are no devices added.
- If you enter an IP address for the non accessible devices that is already used by a router interface.
- If you enter an IP address for the non accessible devices that is already used as a global IP address for an accessible device.
- If you enter local IP address for a device that falls outside the subnet for the LAN interface it connects to.

Easy VPN Remote Wizard: Interfaces and Connection Settings

In this window, you specify the interfaces that will be used in the Easy VPN configuration.

Field Reference

Table 12-4 describes the fields in th is screen.

Table 12-4   *Interfaces and Connection Settings Fields*

Element	Description
Interfaces	
Choose the inside and outside interfaces in this box.	
Check boxes	Check the inside (LAN) interfaces that serve the local networks that you want to include in this Easy VPN configuration. You can choose multiple inside interfaces, with the following restrictions:
	• If you choose an interface that is already used in another Easy VPN configuration, you are told that an interface cannot be part of two Easy VPN configurations.
	• If you choose interfaces that are already used in a VPN configuration, you are informed that the Easy VPN configuration you are creating cannot coexist with the existing VPN configuration. You will be asked if you want to remove the existing VPN tunnels from those interfaces and apply the Easy VPN configuration to them.
	• An existing interface does not appear in the list of interfaces if it cannot be used in an Easy VPN configuration. For example, loopback interfaces configured on the router do not appear in this list.
	• An interface cannot be designated as both an inside and an outside interface.
	Up to three inside interfaces are supported on Cisco 800 and Cisco 1700 series routers. You can remove interfaces from an Easy VPN configuration in the Edit Easy VPN Remote window.
Interface List	In the Interfaces list, choose the outside interface that connects to the Easy VPN server or concentrator.
	✎
	Note Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Connection Settings	

Table 12-4   *Interfaces and Connection Settings Fields*

Element	Description
Automatically	With the automatic setting, the VPN tunnel is established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect or Disconnect button is disabled when this Easy VPN connection is chosen.
Manually	With the manual setting, you must click the **Connect** or **Disconnect** button in the Edit Easy VPN Remote window to establish or take down the tunnel, but you will have full manual control over the tunnel in the Edit Easy VPN Remote window. Additionally, if a security association (SA) timeout is set for the router, you will have to manually reestablish the VPN tunnel whenever a timeout occurs. You can change SA timeout settings in the VPN Components VPN Global Settings window.
When there is traffic from local networks (interesting traffic)	With the traffic-based setting, the VPN tunnel is established whenever outbound local (LAN side) traffic is detected. **Note** The option for traffic-based activation appears only if supported by the Cisco IOS image on your router.

Easy VPN Remote Wizard: Server Information

The information entered in this window identifies the Easy VPN tunnel, the Easy VPN server or concentrator that the router will connect to, and the way you want traffic to be routed in the VPN.

Field Reference

Table 12-5 describes the fields in this screen.

Table 12-5   Server Information Fields

Element	Description
Easy VPN Servers	
Easy VPN Server 1	Enter the IP address or the hostname of the primary Easy VPN server or concentrator to which the router will connect. If you enter a hostname, there must be a Domain Name System (DNS) server on the network that can resolve the hostname to the correct IP address for the peer device.
Easy VPN Server 2	The Easy VPN Server 2 field appears when the Cisco IOS image on the router supports Easy VPN Remote Phase III. This field does not appear when the Cisco IOS image does not support Easy VPN Remote Phase III.
	Enter the IP address or the hostname of the secondary Easy VPN server or concentrator to which the router will connect. If you enter a hostname, there must be a DNS server on the network that can resolve the hostname to the correct IP address for the peer device.
Mode of operation with no identical addressing	
Client	Choose **Client** if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN, or reach them directly.
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
	Consult with the administrator of the Easy VPN server or concentrator before choosing this setting.

Table 12-5   Server Information Fields (continued)

Element	Description
	If you choose Network Extension, you can enable remote management of the router by checking the box to request a server-assigned IP address for your router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is known as **Network Extension Plus** ✎ **Note** If the router is not running a Cisco IOS image that supports Easy VPN Remote Phase IV or later, you will not be able to set Network Extension Plus.
Mode of operation with overlapping address space and local devices needing to be reached	
If you clicked **Yes** in the Client IP Addressing section of the Network Information screen, and also clicked **Yes** in the Device Reachability section, the router is automatically configured for Network Extension mode.	
Have the server assign an IP address to manage my router remotely	Check this box if you want the Easy VPN server to assign an IP address to the router so that it can manage the router Easy VPN operation remotely.
Mode of operation with overlapping address space but no devices needing to be reached	
If you clicked **Yes** in the Client IP Addressing section of the Network Information screen, but clicked **No** in the Device Reachability section, the router is automatically configured for Client mode. The Easy VPN server automatically assigns the router an IP address so that it can manage the router Easy VPN operation remotely. All devices on the local network will share this IP address when communicating with other devices on the corporate network.	

Easy VPN Remote Wizard: Authentication

Use this window to specify security for the Easy VPN Remote tunnel.

Field Reference

Table 12-6 describes the fields in this screen.

Table 12-6   *Authentication Screen Fields*

Element	Description
Device Authentication	
Authentication	Choose **Digital Certificate** or **Preshared Key**.
Digital Certificate	If you choose digital certificate, a digital certificate must be configured on the router to use. ✎ **Note** The Digital Certificates option is available only if supported by the Cisco IOS image on your router.
Preshared Key	If you choose **Preshared Key** in the authentication field, you must supply a user group name as well as the preshared key.
User Group	Enter the IPSec group name. The group name must match the group name defined on the VPN concentrator or server. Obtain this information from your network administrator.
Key	Enter the IPSec group key. The group key must match the group key defined on the VPN concentrator or server. Obtain this information from your network administrator.
Reenter key	Reenter the key to confirm its accuracy.
User Authentication	
User authentication (XAuth) appears in this window if the Cisco IOS image on the router supports Easy VPN Remote Phase III. If user authentication does not appear, it must be configured from the router command-line interface.	
From PC browser when browsing	User authentication will be performed in the web browser. This option appears only if supported by the Cisco IOS image on your router.
From router console or SDM	User authentication will be performed from the router console, or from Cisco SDM.

Table 12-6   Authentication Screen Fields

Element	Description
Save XAuth Credentials to this router	The Easy VPN server may use XAuth to authenticate the router. If the server allows the save password option, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established by this option. Enter the username and password provided by the Easy VPN server administrator, and then reenter the password to confirm its accuracy. The information is saved in the router configuration file and used each time the tunnel is established. ⚠ **Caution** Storing the XAuth username and password in router memory creates a security risk, because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Additionally, Cisco SDM cannot itself determine whether the Easy VPN server allows the save password option. You must determine whether the server allows this option. If the server does not allow this option, you should not create a security risk by entering the information here.
Username	Enter the username required for authentication.
Password	Enter the password required for authentication.
Reenter password	Reenter the password to confirm accuracy.

Easy VPN Remote Wizard: Summary of Configuration

This window shows you the Easy VPN configuration that you have created, and it allows you to save the configuration. A summary similar to the following appears:

```
Easy VPN tunnel name:test1
Easy VPN server: 222.28.54.7
Group: myCompany
Key: 1234
```

```
Control: Auto
Mode: Client
Outside Interface: BVI222
Inside Interfaces: Dialer0
```

You can review the configuration in this window and click the **Back** button to change any items.

Clicking the **Finish** button writes the information to the router's running configuration, and, if the tunnel has been configured to operate in automatic mode, the router attempts to contact the VPN concentrator or server.

If you want to change the Easy VPN configuration at a later time, you can make the changes in the Edit Easy VPN Remote window.

> **Note**   In many cases, your router establishes communication with the Easy VPN server or concentrator after you click **Finish**, or after you click **Connect** in the Edit Easy VPN Remote window or VPN Connections windows. However, if the device has been configured to use XAuth, it challenges the router for a username and password. When this happens, you must first supply a Secure Shell (SSH) login ID and password to log on to the router and then provide the XAuth login and password for the Easy VPN server or concentrator. You must follow this process when you click **Finish** and the configuration is delivered to the router, and when you disconnect and then reconnect the tunnel in the Edit Easy VPN Remote window. Find out whether XAuth is used, and determine the required username and password.

Test VPN Connectivity

If you choose to test the VPN connection you have just configured, the results of the test are shown in another window.

Administering Easy VPN Remote Connections

Use Cisco SDM to edit Easy VPN Remote connection settings, reset connections, and delete connections. You can use the Easy VPN Remote Edit screens to create an Easy VPN Remote connection, but it is recommended that you use the wizard to do so.

This section contains the followint topics:

Editing an Existing Easy VPN Remote Connection

Follow these steps to edit an existing Easy VPN Remote connection:

Step 1 On the Cisco SDM toolbar, click **Configure**.

Step 2 On the Cisco SDM category bar, click **VPN**.

Step 3 In the VPN tree, choose **Easy VPN Remote**.

Step 4 Click the **Edit Easy VPN Remote** tab.

Step 5 Select the Easy VPN Remote connection that you want to edit.

Step 6 Click **Edit**.

Step 7 Modify settings in the **Edit Easy VPN Remote** dialog tabs.

Step 8 Click **OK** to send the changes to the router and close the dialog.

Creating a New Easy VPN Remote Connection

You can create a new Easy VPN Remote connection using the Easy VPN Remote Edit screens.

Follow these steps to create a new Easy VPN Remote connection:

Step 1 On the Cisco SDM toolbar, click **Configure**.

Step 2 On the Cisco SDM category bar, click **VPN**.

Step 3   In the VPN tree, choose **Easy VPN Remote**.

Step 4   Click the **Edit Easy VPN Remote** tab.

Step 5   Click **Add**.

Step 6   Make settings in the **Add Easy VPN Remote** dialog tabs.

Step 7   Click **OK** to send the changes to the router and close the dialog.

Deleting an Easy VPN Remote Connection

Follow these steps to delete an Easy VPN Remote connection:

Step 1   On the Cisco SDM toolbar, click **Configure**.

Step 2   On the Cisco SDM category bar, click **VPN**.

Step 3   In the VPN tree, choose **Easy VPN Remote**.

Step 4   Click the **Edit Easy VPN Remote** tab.

Step 5   Select the Easy VPN Remote connection that you want to delete.

Step 6   Click **Delete**.

Step 7   Confirm the deletion by clicking **OK** in the displayed message screen.

Resetting an Established Easy VPN Remote Connection

Follow these steps to reset an established Easy VPN Remote connection:

Step 1   On the Cisco SDM toolbar, click **Configure**.

Step 2   On the Cisco SDM category bar, click **VPN**.

Step 3   In the VPN tree, choose **Easy VPN Remote**.

Step 4   Click the **Edit Easy VPN Remote** tab.

Step 5   Select the Easy VPN Remote connection that you want to reset.

Step 6   Click **Reset Connection**. The status window that is displayed reports the success or failure of the reset.

Connecting to an Easy VPN Server

Follow these steps to connect to an Easy VPN Remote server:

Step 1   On the Cisco SDM toolbar, click **Configure**.

Step 2   On the Cisco SDM category bar, click **VPN**.

Step 3   In the VPN tree, choose **Easy VPN Remote**.

Step 4   Click the **Edit Easy VPN Remote** tab.

Step 5   Select an Easy VPN Remote connection.

Step 6   Click **Connect** to complete the connection to the configured Easy VPN Server.

Connecting other Subnets to the VPN Tunnel

To allow subnets not directly connected to your router to use the tunnel, follow these steps:

Step 1   In the Network Extensions Options window, check **Configure Multiple Subnets**.

Step 2   Choose **Enter the subnets** and add the subnets and network masks to the list, or choose **Select an ACL**.

Step 3   To enter the subnets manually, click the **Add** button and enter the subnet address and mask. Cisco SDM will generate an ACL automatically.

> **Note**   The subnets you enter must *not* be directly connected to the router.

Step 4   To add an existing ACL, enter its name or choose it from the drop-down list.

Step 5   Click **OK** to close the dialog.

Administering Easy VPN Remote Reference

The following topics describe the Edit Easy VPN Remote screens:

- Edit Easy VPN Remote
- Add or Edit Easy VPN Remote
- Add or Edit Easy VPN Remote: General Settings
- Network Extension Options
- Add or Edit Easy VPN Remote: Easy VPN Settings
- Add or Edit Easy VPN Remote: Authentication Information
- Add or Edit Easy VPN Remote: Easy VPN Client Phase III Authentication
- Add or Edit Easy VPN Remote: Interfaces and Connections
- Add or Edit Easy VPN Remote: Identical Addressing
- Easy VPN Remote: Add a Device
- Enter SSH Credentials
- XAuth Login Window

Edit Easy VPN Remote

Easy VPN connections are managed from this window. An Easy VPN connection is a connection configured between an Easy VPN client and an Easy VPN server or concentrator to provide for secure communications with other networks that the server or concentrator supports.

The list of connections displays information about the configured Easy VPN Remote connections.

Field Reference

Table 12-7 describes the fields and buttons in this screen.

Table 12-7   Edit Easy VPN Remote Fields

Element	Description
Add	Click **Add** to create a new Easy VPN Remote connection.
Edit	Choose an Easy VPN Remote connection, and click **Edit** to modify connection settings.
Delete	Choose an Easy VPN Remote connection, and click **Delete** to delete the connection.
Reset Connection	Choose an Easy VPN Remote connection, and click **Reset Connection** to clear the current security association (SA) and create a new one to reset the connection.
Test Tunnel	Choose an Easy VPN Remote connection, and click **Test Tunnel** to send data through the VPN tunnel. Cisco SDM displays a message indicating the results of the test.
Connect or Disconnect or Login	The name of this button changes based on the status of the chosen Easy VPN Remote connection.
	This button is labeled Connect if all of the following are true: • The connection uses manual tunnel control. • The tunnel is down. • The XAuth response is *not* set to be requested from a PC browser session. Click **Connect** to establish the connection. This button is labeled Disconnect if all of the following are true: • The connection uses manual tunnel control. • The tunnel is up. • The XAuth response is *not* set to be requested from a PC browser session. Click **Disconnect** to terminate the connection.

Table 12-7   Edit Easy VPN Remote Fields

Element	Description
	This button is labeled Login if all of the following are true:
	• The Easy VPN server or concentrator being connected to uses XAuth.
	• The XAuth response is set to be requested from Cisco SDM or the router console.
	• The tunnel is waiting for XAuth credentials (the connection has been initiated).
	Click **Login** to login to the Easy VPN server and establish the connection.
	If the connection is set to automatic or traffic-based tunnel control, this button is disabled.
Status	
(green icon)	The connection is up. When an Easy VPN connection is up, the Disconnect button enables you to deactivate the connection if manual tunnel control is used.
(red icon)	The connection is down. When an Easy VPN connection is down, the Connect button enables you to activate the connection if manual tunnel control is used.
(yellow icon)	The connection is being established.
	Xauth Required—The Easy VPN server or concentrator requires an XAuth login and password. Use the Login button to enter the login ID and password and establish the connection.
	Configuration Changed—The configuration for this connection has been changed, and needs to be delivered to the router. If the connection uses manual tunnel control, use the Connect button to establish the connection.
Name	The name given to this Easy VPN connection.

Table 12-7   Edit Easy VPN Remote Fields

Element	Description
Mode	Either **client** or **network extension**. In client mode, the VPN concentrator or server assigns a single IP address to all traffic coming from the router; devices outside the LAN have no direct access to devices on the LAN. In network extension mode, the VPN concentrator or server does not substitute IP addresses, and it presents a full routable network to the peers on the other end of the VPN connection.
Details	
Choose an Easy VPN Remote connection from the list to see the values of the following settings for that connection.	
Authentication	Digital certificates or preshared key. The preshared key option shows the user group sharing the key.
Outside Interface	This is the interface that connects to the Easy VPN server or concentrator.
Inside Interfaces	These are the inside interfaces included in this Easy VPN connection. All hosts connected to these interfaces are part of the VPN.
Easy VPN Server	The names or IP addresses of the Easy VPN servers or concentrators. If the Cisco IOS image on your router supports Easy VPN Remote Phase III, you can identify two Easy VPN servers or concentrators during configuration using Cisco SDM.
Multiple Subnet Support	The addresses of subnets which are not directly connected to the router but which are allowed to use the tunnel. An ACL defines the subnets allowed to use the tunnel.

Table 12-7   Edit Easy VPN Remote Fields

Element	Description
Tunnel Activation	The value is Auto, Manual, or traffic-based.
	If the connection is configured with the Manual setting, you must click **Connect** to establish the tunnel, but you can start or stop the tunnel at any time by clicking **Connect** or **Disconnect**.
	If the connection is configured with the Auto setting, the VPN tunnel is established automatically when the Easy VPN configuration is delivered to the router configuration file. However, the Connect or Disconnect button is not enabled for this connection.
	If the connection is configured with the traffic-based setting, the VPN tunnel is established automatically when inside traffic qualifies for outside routing. However, the Connect or Disconnect button is not enabled for this connection.
Backup Connection	A backup Easy VPN remote connection that has been set up. Backup connections are configured in the Cisco SDM Interfaces and Connections task.
XAuth Response Method	If XAuth is enabled, the Item Value column shows one of the following about how the XAuth credentials are sent: • They must be entered from Cisco SDM or the router console. • They must be entered from a PC browser when browsing. • The credentials are automatically sent because they have been saved on the router.
Identical Addressing Interface	If identical addressing is configured, the Item Value column displays the word Configured," and the name, IP address, and number of subnet bits for the interface, for example, Loopback1 (20.20.20.1/24).
Split DNS	If split DNS is configured, the Item Value column displays the word Enabled, and the following information: • Domain names sent to corporate DNS servers • Corporate DNS servers pushed from Server • Internet DNS servers Multiple values are separated by commas.

Add or Edit Easy VPN Remote

Use this window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note   This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase II.

The Cisco Easy VPN Remote feature implements the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Note   • If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and then reconnect the tunnel. Find out whether XAuth is used and the required username and password.

   • If the router uses Secure Shell (SSH) you must enter the SSH login and password the first time you establish the connection.

Field Reference

Table 12-8 describes the fields in this screen.

Table 12-8   Add or Edit Easy VPN Remote Fields

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Mode]	
Client	Choose **Client** if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.

Table 12-8   ***Add or Edit Easy VPN Remote Fields***

Element	Description
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
Tunnel Control	
Auto	Choose **Auto** if you want the VPN tunnel to be established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect and Disconnect buttons are disabled when this Easy VPN connection is chosen.
Manual	Choose **Manual** if you want to control when the VPN tunnel is established and terminated. You must click the **Connect** button in the Edit Easy VPN Remote window to establish the tunnel. The Connect and Disconnect buttons are enabled whenever you choose a VPN connection with the Manual tunnel control setting.
Easy VPN Concentrator or Server	Specify the name or the IP address of the VPN concentrator or server that the router connects to. Choose **IP address** if you are going to provide an IP address or choose **Hostname** if you are going to provide the hostname of the concentrator or server. Then specify the appropriate value in the field underneath. If you specify a hostname, there must be a DNS server on the network that can resolve the hostname to the proper IP address. If you enter an IP address, use standard dotted decimal format, for example, 172.16.44.1.
Group	
Group Name]	Enter the IPSec group name. The group name must match the group name defined on the VPN concentrator or server. Obtain this information from your network administrator.

Table 12-8   *Add or Edit Easy VPN Remote Fields*

Element	Description
Group Key	Enter the IPSec group password. The group password must match the group password defined on the VPN concentrator or server. Obtain this information from your network administrator.
Confirm Key	Reenter the group password to confirm.

Interfaces	
Outside Interface Toward Server or Concentrator	Choose the interface that has the connection to the Easy VPN server or concentrator. **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Inside Interfaces	Specify the inside interfaces to include in this Easy VPN configuration. All hosts connected to these interfaces will be part of the VPN. As many as three inside interfaces are supported on Cisco 800 series and Cisco 1700 series routers. **Note** An interface cannot be designated as both an inside interface and an outside interface.

Add or Edit Easy VPN Remote: General Settings

Use this Window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note   This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase IV.

The Cisco Easy VPN Remote feature implements the Cisco Unity Client protocol, which allows most VPN parameters to be defined on a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Field Reference

Table 12-9 describes the fields in this screen.

Table 12-9   *Easy VPN Remote General Settings Fields*

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Servers	You can specify up to ten Easy VPN servers by IP address or hostname, and you can order the list to specify which servers the router will attempt to connect to first.
	Click **Add** to specify the name or the IP address of a VPN concentrator or server for the router to connect to, and then enter the address or hostname in the window displayed.
	Click **Delete** to delete the specified IP address or hostname.
	Click **Move Up** to move the specified server IP address or hostname up in the list. The router attempts to contact routers in the order in which they appear in this list.
	Click **Move Down** to move the specified IP address or hostname down the list.
Mode	
Client	Choose **Client** mode if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.

Table 12-9   Easy VPN Remote General Settings Fields

Element	Description

Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
	
	• Enable remote management and troubleshooting of your router.
	
	  You can enable remote management of the router by checking the box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.
	
	Consult the administrator of the Easy VPN server or concentrator before you choose this setting.
	
	If you choose Network Extension, you also have the capability to:
	
	• Allow subnets not directly connected to the router to use the tunnel.
	
	  To allow subnets not directly connected to your router to use the tunnel, click the **Options** button and configure the network extension options.
	
	• Enable remote management and troubleshooting of your router.
	
	  You can enable remote management of the router by checking the box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.

Have the server assign an IP address to manage my router remotely.	Check this box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.

Network Extension Options

To allow subnets not directly connected to your router to use the tunnel, enter the subnets in this screen, or enter an ACL that defines the subnets you want to allow.

Field Reference

Table 12-10 describes the fields in this screen.

Table 12-10   Network Extension Options Fields

Element	Description
Configure Multiple Subnets	Check **Configure Multiple Subnets** to enable the other fields in this screen.
Enter the subnets. SDM will create the necessary ACL.	Check this option to enter each subnet and subnet mask manually. Click **Add** to add an entry to the list. Click **Delete** to remove the selected entry.
Select an ACL	Check **Select an ACL** to use an ACL to define the subnets. If you know the name or number of the ACL enter it in the field. Or, click the button to the right of the field, and select an existing ACL or create a new ACL. To remove an ACL association in this screen, click the button and choose **None** (**clear rule association**).

Add or Edit Easy VPN Remote: Easy VPN Settings

Use this window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note   This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase III.

The Cisco Easy VPN Remote feature implements The Cisco Unity Client protocol, which allows most VPN parameters to be defined on a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Field Reference

Table 12-11 describes the fields in this screen.

Table 12-11   Easy VPN Settings Fields

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Mode	
Client	Choose **Client** mode if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
	Consult the administrator of the Easy VPN server or concentrator before you choose this setting.
Tunnel Control	
Auto	Choose **Auto** if you want the VPN tunnel to be established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect and Disconnect buttons are disabled when this Easy VPN connection is chosen.
Manual	Choose **Manual** if you want to control when the VPN tunnel is established and terminated. You must click the **Connect** button in the Edit Easy VPN Remote window to establish the tunnel. The Connect and Disconnect buttons are enabled whenever you choose a VPN connection with the Manual tunnel control setting.

Servers

You can specify up to ten Easy VPN servers by IP address or hostname, and you can order the list to specify which servers the router will attempt to connect to first.

Table 12-11 *Easy VPN Settings Fields*

Element	Description
Add	Click **Add** to specify the name or the IP address of a VPN concentrator or server for the router to connect to; then enter the address or hostname in the window displayed.
Delete	Click **Delete** to delete the chosen server IP address or hostname.
Move Up	Click **Move Up** to move the specified server IP address or hostname up in the list. The router attempts to contact routers in the order in which they appear in this list.
Move Down	Click **Move Down** to move the specified IP address or hostname down the list.
Outside Interface Toward Server or Concentrator	Choose the interface that has the connection to the Easy VPN server or concentrator. ✎ **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Inside Interfaces	Specify the inside interfaces to include in this Easy VPN configuration. All hosts connected to these interfaces will be part of the VPN. As many as three inside interfaces are supported on Cisco 800 series and Cisco 1700 series routers. ✎ **Note** An interface cannot be designated as both an inside and an outside interface.

Add or Edit Easy VPN Remote: Authentication Information

Use this window to enter the information required for the router to be authenticated by the Easy VPN server or concentrator.

Field Reference

Table 12-12 describes the fields in this screen.

Table 12-12   Authentication Information Fields

Element	Description
Device Authentication	
Digital Certificate.	If you choose digital certificate, a digital certificate must be configured on the router to use. ✎ **Note** The Digital Certificates option is available only if supported by the Cisco IOS image on your router.
Preshared Key	Choose Preshared Key to use the IKE key value given to you by your network administrator. Obtain the IPSec group name and IKE key value from your network administrator. The group name must match the group name defined on the VPN concentrator or server.
Group Name	Enter the IPSec groupname given to you by your network administrator. The group name must match the group name defined on the VPN concentrator or server. This field only appears if Preshared Key is chosen.
Current Key	The Current Key field displays asterisks (*) if there is a current IKE key value. This field contains the value <None> if no key has been configured. This field only appears if Preshared Key is chosen.
New Key	Enter the new IKE key value given to you by your network administrator. This field only appears if Preshared Key is chosen.
Reenter Key	Reenter the new key to confirm accuracy. If the values in the New Key and Reenter Key fields are not the same, Cisco SDM prompts you to reenter the key values. This field only appears if Preshared Key is chosen
User Authentication	

If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and reconnect the tunnel. Find out whether XAuth is used, and obtain the required username and password.

Table 12-12   Authentication Information Fields

Element	Description
From PC	Choose **From PC** if you will enter the credentials in a web browser window. ✎ **Note** This option appears only if supported by the Cisco IOS image on your router.
From this router	Choose **From this router** if you will enter the credentials from the router command line interface or from Cisco SDM.
Save Credentials	If the server allows passwords to be saved, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established. The information is saved in the router configuration file and used each time the tunnel is established. Choose **Save Credentials** to save the username and password to the router configuration file. ⚠ **Caution** Storing the XAuth username and password in router memory creates a security risk because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Also, Cisco SDM cannot itself determine whether the server allows passwords to be saved. You must determine whether the server allows this option. If the server does not allow passwords to be saved, you should not create a security risk by entering the information here.
Username	Enter the username you have been given by the server administrator.
Current Password	The Current Password field displays asterisks (*) if there is a configured password. This field contains the value <None> if no password has been configured.

Table 12-12   Authentication Information Fields

Element	Description
New Password	Enter the new password given to you by the server administrator.
Reenter Password	Reenter the new password to confirm accuracy. If the values in the New Password and Reenter Password fields are not the same, Cisco SDM prompts you to reenter the password values.

Add or Edit Easy VPN Remote: Easy VPN Client Phase III Authentication

This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase III. If the image supports Easy VPN Client Phase II, a different window appears.

Use this window to enter the information required for the router to be authenticated by the Easy VPN server or concentrator.

Field Reference

Table 12-13 describes the fields in this screen.

Table 12-13   Authentication Information Fields

Element	Description
Device Authentication	
Group Name	Enter the IPSec groupname given to you by your network administrator. The group name must match the group name defined on the VPN concentrator or server.
Current Key	The Current Key field displays asterisks (*) if there is a current IKE key value. This field contains the value <None> if no key has been configured.
New Key	Enter the new IKE key value given to you by your network administrator.
Reenter Key	Reenter the new key to confirm accuracy. If the values in the New Key and Reenter Key fields are not the same, Cisco SDM prompts you to reenter the key values.

Table 12-13   Authentication Information Fields

Element	Description
User Authentication	
If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and reconnect the tunnel. Find out whether XAuth is used, and obtain the required username and password.	
From PC	Choose **From PC** if you will enter the credentials in a web browser window. **Note** This option appears only if supported by the Cisco IOS image on your router.
From this router	Choose **From this router** if you will enter the credentials from the router command line interface or from Cisco SDM.
Save Credentials	If the server allows passwords to be saved, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established. The information is saved in the router configuration file and used each time the tunnel is established. Choose **Save Credentials** to save the username and password to the router configuration file. **Caution** Storing the XAuth username and password in router memory creates a security risk because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Also, Cisco SDM cannot itself determine whether the server allows passwords to be saved. You must determine whether the server allows this option. If the server does not allow passwords to be saved, you should not create a security risk by entering the information here.
Username	Enter the username you have been given by the server administrator.

Table 12-13   Authentication Information Fields

Element	Description
Current Password	The Current Password field displays asterisks (*) if there is a configured password. This field contains the value <None> if no password has been configured.
New Password	Enter the new password given to you by the server administrator.
Reenter Password	Reenter the new password to confirm accuracy. If the values in the New Password and Reenter Password fields are not the same, Cisco SDM prompts you to reenter the password values.

Add or Edit Easy VPN Remote: Interfaces and Connections

Identify the inside and outside interfaces, and specify how the VPN tunnel is brought up in this screen.

Field Reference

Table 12-14 describes the fields in this screen.

Table 12-14   Interfaces and Connection Settings Fields

Element	Description
Interfaces	
Check boxes	Check the inside (LAN) interfaces that serve the local networks that you want to include in this Easy VPN configuration. You can choose multiple inside interfaces, with the following restrictions:
	• If you choose an interface that is already used in another Easy VPN configuration, you are told that an interface cannot be part of two Easy VPN configurations.
	• If you choose interfaces that are already used in a VPN configuration, you are informed that the Easy VPN configuration you are creating cannot coexist with the existing VPN configuration. You will be asked if you want to remove the existing VPN tunnels from those interfaces and apply the Easy VPN configuration to them.

Table 12-14   *Interfaces and Connection Settings Fields*

Element	Description
	• An existing interface does not appear in the list of interfaces if it cannot be used in an Easy VPN configuration. For example, loopback interfaces configured on the router do not appear in this list. • An interface cannot be designated as both an inside and an outside interface. Up to three inside interfaces are supported on Cisco 800 and Cisco 1700 series routers. You can remove interfaces from an Easy VPN configuration in the Edit Easy VPN Remote window.
Interface list	In the Interfaces list, choose the outside interface that connects to the Easy VPN server or concentrator. **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface
Virtual Tunnel Interface	Check this option if you want to use a Virtual Tunnel Interface (VTI) for this connection. If the VTIs in the list are used by other VPN connections, click **Add** to create a new one.
Connection Settings	
Auto	Choose **Auto** to have the router establish the VPN tunnel automatically when the Easy VPN configuration is delivered to the router configuration file. You will not be able to control the tunnel manually using the Connect or Disconnect button. These buttons are disabled when this setting is chosen.

Table 12-14   Interfaces and Connection Settings Fields

Element	Description
Manual	Choose **Manual** if you want to bring up and shut down the VPN tunnel manually. With the manual setting, you must click the **Connect** or **Disconnect** button in the Edit Easy VPN Remote screen to establish or take down the tunnel. Additionally, if a security association (SA) timeout is set for the router, you will have to manually reestablish the VPN tunnel whenever a timeout occurs. You can change SA timeout settings in the VPN Components VPN Global Settings window.
Interesting Traffic	Choose **Interesting Traffic** to establish the VPN tunnel whenever outbound local (LAN side) traffic is detected. The Connect or Disconnect button is disabled when you choose this Easy VPN connection setting. **Note** The Interesting Traffic option appears only if supported by the Cisco IOS image on your router.

Add or Edit Easy VPN Remote: Identical Addressing

In this screen, enter the information needed to configure identical addressing. Identical addressing enables remote networks to reach local devices that have IP addresses that might overlap with addresses in remote networks.

Field Reference

Table 12-15   Identical Addressing Tab Fields

Element	Description
Configure identical addressing	Check **Configure identical addressing** if there are devices on the local network with IP addresses that might overlap with addresses in remote networks in your organization. You must check this box to enable the other controls in this screen.
Loopback Interface	
Loopback Interface	Click the down arrow to select an existing loopback interface. If no loopback interfaces are configured, click **Add**.

Table 12-15   *Identical Addressing Tab Fields (continued)*

Element	Description
Add	Clicking **Add** displays the dialog that enables you to configure a loopback interface.
Enable split tunneling	Split tunneling enables the router to only use the VPN tunnel to send traffic to network addresses given to it by the Easy VPN server and to send other traffic through the Internet. To enable the router to use this feature, click **Enable split tunneling**.
Accessible Devices	
Device Local IP	The local IP address of a device that is identified as a device that must be reached by other networks.
Device Global IP	The global IP address given to a device that is identified as a device that must be reached by other networks. Because the global IP address for each device must be routable from the Easy VPN server, you must obtain these addresses from the Easy VPN server administrator. Each IP address must be on the same subnet, and one address must be reserved for use by non accessible devices on the local network.
Add	To add the local IP address and global IP address of a device, click **Add**.
Edit	To change the IP address information for a device, choose an entry and click **Edit**.
Delete	To remove an entry for an accessible device, choose the entry and click **Delete**.

Warning Messages

Cisco SDM displays a warning message when you click **OK** if it detects any of the following problems:

- There are no devices added.

- If you enter an IP address for the non accessible devices that is already used by a router interface.

- If you enter an IP address for the non accessible devices that is already used as a global IP address for an accessible device.

- If you enter local IP address for a device that falls outside the subnet for the LAN interface it connects to.

- If you chose client mode in the General tab. Identical addressing only works with network extension mode.

- If you did not choose a virtual tunnel interface in the Interfaces and Connections tab.

Easy VPN Remote: Add a Device

Enter the local IP address and global IP address information for a device in this screen. The global IP address is an IP address that can be used to identify the device to other networks.

Field Reference

Table 12-16 describes the fields in this screen.

Table 12-16   Add a Device Fields

Element	Description
Local IP Address	Enter the local IP address of the device that must be reached.
Global IP Address	Enter the global IP address that you want to use for this device. The address you use must be routable from the Easy VPN server.

Enter SSH Credentials

If the router uses Secure Shell (SSH), you must to enter the SSH login and password the first time you establish the connection. Use this window to enter SSH or Telnet login information.

Field Reference

Table 12-17 describes the fields in this screen.

Table 12-17   Enter SSH Credentials Fields

Element	Description
Please Enter the Username	Enter the SSH or Telnet account username that you will use to log in to this router.
Please Enter the Password	Enter the password associated with the SSH or Telnet account username that you will use to log in to this router.

XAuth Login Window

This window appears when the Easy VPN server requests extended authentication. Respond to the challenges by entering the information requested, such as the account username, password, or any other information, to successfully establish the Easy VPN tunnel. If you are unsure about the information that should be provided, contact your VPN administrator.

Other Procedures

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Edit an Existing Easy VPN Connection?

To edit an existing Easy VPN remote connection, follow these steps:

Step 1   From the left frame, choose **VPN**.

Step 2   In the VPN tree, choose **Easy VPN Remote**.

Step 3   Click the **Edit Easy VPN Remote** tab and choose the connection that you want to edit.

Step 4   Click **Edit.**

The Edit Easy VPN Remote window appears.

Step 5 In the Edit Easy VPN Remote window, click the tabs to display the values that you want to change.

Step 6 When you have finished making changes, click **OK**.

How Do I Configure a Backup for an Easy VPN Connection?

To configure a backup for an Easy VPN Remote connection, your router must have an ISDN, async, or analog modem interface available for the backup.

If the ISDN, async, or analog modem interface has not been configured, follow these steps:

Step 1 From the left frame, click **Interfaces and Connections**.

Step 2 Click the **Create Connection** tab.

Step 3 Choose an ISDN, async, or analog modem interface from the list.

Step 4 Click the **Create New Connection** button and use the wizard to configure the new interface.

Step 5 In the appropriate wizard window, set the new interface as a backup for an Easy VPN Remote connection.

If the ISDN, async, or analog modem interface has been configured, follow these steps:

Step 1 From the left frame, click **Interfaces and Connections**.

Step 2 Click the **Edit Interface/Connection** tab.

Step 3 Choose an ISDN, async, or analog modem interface from the list of configured interfaces.

Step 4 Click the **Edit** button.

Step 5 Click the **Backup** tab and configure the backup for an Easy VPN Remote connection.

Step 6   When you have finished configuring the backup, click **OK**.

Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients. The feature allows a remote end user to communicate using IP Security (IPSec) with anyCisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

The following link provides general information on the Cisco Easy VPN solution, and other links for more specific information:

http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html

This chapter contains the following sections:

- Creating an Easy VPN Server Connection
- Editing Easy VPN Server Connections

Creating an Easy VPN Server Connection

Use theCisco SDM Easy VPN Server wizard to create an Easy VPN Server connection on the router.

Complete these steps to configure an Easy VPN Server connection using the Easy VPN Server wizard:

Step 1 If you want to review the Cisco IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2 In the Cisco SDM toolbar, click **Configure**.

Step 3 In the Cisco SDM taskbar, click **VPN**.

Step 4 In the VPN tree, click Easy VPN Server.

Step 5 In the Create Easy VPN Server tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco SDM either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 6 Click **Launch Easy VPN Server Wizard** to begin configuring the connection.

Step 7 Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 8 Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 9 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco SDM tests the connection and displays the test results in another screen.

Step 10 To send the configuration to the router, click **Finish**.

Step 11 If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **OK** to send the configuration to the router, or click **Cancel** to discard it. If you did not make this setting, clicking Finish sends the configuration to the router.

Create an Easy VPN Server Reference describes the configuration screens you use to create an Easy VPN server connection.

Create an Easy VPN Server Reference

The topics in this section describe the configuration screens:

- Create an Easy VPN Server
- Welcome to the Easy VPN Server Wizard
- Interface and Authentication
- Group Authorization and Group Policy Lookup
- User Authentication (XAuth)
- User Accounts for XAuth
- Add RADIUS Server
- Group Authorization: User Group Policies
- General Group Information
- DNS and WINS Configuration
- Split Tunneling
- Client Settings
- Choose Browser Proxy Settings
- Add or Edit Browser Proxy Settings
- User Authentication (XAuth)
- Client Update
- Add or Edit Client Update Entry
- Cisco Tunneling Control Protocol
- Summary
- Browser Proxy Settings

Create an Easy VPN Server

This wizard will guide you through the necessary steps to configure an Easy VPN Server on this router.

Field Reference

Table 13-1 describes the fields in this screen.

Table 13-1   *Create an Easy VPN Server Fields*

Element	Description
Launch the Easy VPN Server Wizard	Click this button to start the wizard.

Welcome to the Easy VPN Server Wizard

This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router.

- Choosing the interface on which the client connections will terminate, and the authentication method used for the server and Easy VPN clients

- Configuring IKE policies

- Configuring an IPSec transform set

- Configuring group authorization and the group policy lookup method

- Configuring user authentication

- Configuring external RADIUS servers

- Configuring policies for remote users connecting to Easy VPN clients

Interface and Authentication

This window lets you choose the interface on which you want to configure the Easy VPN Server.

If you choose an interface that is already configured with a site-to-site IPSec policy, Cisco SDM displays a message that an IPSec policy already exists on the interface. Cisco SDM uses the existing IPSec policy to configure the Easy VPN Server.

If the chosen interface is part of an Easy VPN Remote, GREoIPSec, or DMVPN interface, Cisco SDM displays a message to choose another interface.

Field Reference

Table 13-2 describes the fields in this screen.

Table 13-2   Interface and Authentication Fields

Element	Description
Details	Click this button to obtain details about the interface you choose. The details window shows any access rules, IPSec policies, NAT rules, or inspection rules associated with the interface.
	This button is dimmed when no interface is chosen.
Authentication	Choose one of the following:
	Pre-shared Keys—If you click **Pre-shared Keys**, you must enter a key value when you configure the Add Group Policy general setup window.
	Digital Certificates—If you click **Digital Certificates**, the preshared keys fields does not appear in the Add Group Policy general setup window.
	Both—If you **Both**, entering a key value in the Add Group Policy general setup window is optional.

Group Authorization and Group Policy Lookup

This windowallows you to define a new AAA authorization network method list for group policy lookup or to choose an existing network method list.

Field Reference

Table 13-3 describes the fields in this screen.

Table 13-3   Group Authorization and Policy Lookup Fields

Element	Description
Local Only	This option allows you to create a method list for the local database only.
	When you define an AAA method list for the local database, the router looks at the local database for group authentication.
RADIUS Only	This option allows you to create a method list for a RADIUS database.
RADIUS and Local	This option allows you to create a method list for both RADIUS and local database.
	When you define method lists for both a RADIUS and local database, the router first looks at the RADIUS server and then the local database for group authentication.
Select an existing AAA method list	This option lets you choose an existing AAA method list on the router to use for group authentication.

User Authentication (XAuth)

You can configure user authentication on Easy VPN Server. You can store user authentication details on an external server such as a RADIUS server or a local database or on both. An AAA login authentication method list is used to decide the order in which user authentication details should be searched.

Field Reference

Table 13-4 describes the fields in this screen.

Table 13-4   User Authentication Fields

Element	Description
Local	Click **Local** to add user authentication details to the local database.
RADIUS	Click **RADIUS** if you want to add user authentication details to the database on the RADIUS server.
RADIUS and Local	Click **RADIUS and Local** to add user authentication details for both a RADIUS and local database.
Select an existing AAA Method List	Click **Select an existing AAA Method List** to choose a method list from a list of all method lists configured on the router. The chosen method list is used for extended authentication.
Add User Credentials	Click **Add User Credentials** to add a user account.
Summary	If you choose RADIUS, the Summary box is displayed. It explains how the RADIUS and local databases are used, and that the Easy VPN remote user can be notified when their password has expired. • Notify remote user of password expiration—This option is checked by default. When enabled, the Easy VPN Server notifies the user when their password has expired and prompts them to enter a new password.

User Accounts for XAuth

Add an account for a user you want to authenticate after IKE has authenticated the device.

Field Reference

Table 13-5 describes the fields in this screen.

Table 13-5   User Accounts for XAuth Fields

Element	Description
User Accounts	The user accounts that XAuth will authenticate are listed in this box. The account name and privilege level are visible.
Add Edit	Use these buttons to add and edit user accounts. User accounts can be deleted in the **Additional Tasks > Router Access > User Accounts/View** window. **Note** Existing CLI view user accounts cannot be edited from this window. If you need to edit user accounts, go to **Additional Tasks > Router Access >User Accounts/CLI View**.

Add RADIUS Server

This window lets you add a new RADIUS server or edit or ping an already existing RADIUS server.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-6   Add a RADIUS Server Fields

Element	Description
Add	Add a new RADIUS server.
Edit	Edit an already exiting RADIUS server configuration.
Ping	Ping an already existing RADIUS server or newly configured RADIUS server.

Group Authorization: User Group Policies

This window allows you to add, edit, clone or delete user group policies on the local database.

Field Reference

Table 13-7 describes the fields in this screen.

Table 13-7   User Group Policies Fields

Element	Description
Group Policy List area	
Select	Check the box in this column next to the groups that you want this Easy VPN server connection to serve.
Group Name	Name given to the user group.
Pool	Name of the IP address pool from which an IP address is assigned to a user connecting from this group.
DNS	Domain Name System (DNS) address of the group. This DNS address is "pushed" to the users connecting to this group.
WINS	Windows Internet Naming Service (WINS) address of the group. This WINS address is "pushed" to the users connecting to this group.
Domain Name	Domain name of the group. This domain name is "pushed" to the users connecting to this group.
Split ACL	The access control list (ACL) that represents protected subnets for split tunneling purposes.
Configure Idle Timer	
Idle Timer	Click the **Configure Idle Timer** check box and enter a value for the maximum time that a VPN tunnel can remain idle before being disconnected. Enter hours in the left field, minutes in the middle field, and seconds in the right field. The minimum time allowed is 1 minute. Disconnecting idle VPN tunnels can help the Easy VPN Server run more efficiently by reclaiming unused resources.

General Group Information

This window allows you to configure, edit and clone group polices.

Field Reference

Table 13-8 describes the fields in this screen.

Table 13-8   General Group Information Fields

Element	Description
Please Enter a Name for This Group	Enter the group name in the field provided. If this group policy is being edited, this field is disabled. If you are cloning a group policy, you must enter a new value in this field.
Preshared Key	Enter the preshared key in the fields provided. The **Current key** field cannot be changed. ✎ **Note** You do not have to enter a preshared key if you are using digital certificates for group authentication. Digital certificates are also used for user authentication.
Pool Information	Specifies a local pool of IP addresses that are used to allocate IP addresses to clients. Create a New Pool—Enter the range of IP addresses for the local IP address pool in the IP Address Range field. Select from an Existing Pool—Choose the range of IP addresses from the existing pool of IP addresses. ✎ **Note** This field cannot be edited if there are no predefined IP address pools.
Subnet Mask (Optional)	Enter a subnet mask to send with the IP addresses allocated to clients in this group.
Maximum Connections Allowed	Specify the maximum number of client connections to the Easy VPN Server from this group. Cisco SDM supports a maximum of 5000 connections per group.

DNS and WINS Configuration

This window allows you to specify the Domain Name Service (DNS) and Windows Internet Naming Service (WINS) information.

Field Reference

Table 13-9 describes the fields in this screen.

Table 13-9   *DNS and WINS Fields*

Element	Description
DNS	Enter the primary and secondary DNS server IP address in the fields provided. Entering a secondary DNS server address is optional.
WINS	Enter the primary and secondary WINS server IP address in the fields provided. Entering a secondary WINS server address is optional.
Domain Name	Specify the domain name that should be pushed to the Easy VPN client.

Split Tunneling

This window allows you to enable split tunneling for the user group you are adding.

Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet. For example, all traffic sourced from the client is sent to the destination subnet through the VPN tunnel.

You can also specify which groups of ACLs represent protected subnets for split tunneling.

Field Reference

Table 13-10 describes the fields in this screen.

Table 13-10   *Split Tunneling Fields*

Element	Description
Enable Split Tunneling	This box allows you to add protected subnets and ACLs for split tunneling.
	• Enter the Protected Subnets—Add or remove the subnets for which the packets are tunneled from the VPN clients.
	• Choose the Split Tunneling ACL—Choose the ACL to use for split tunneling.
Split DNS	Enter the Internet domain names that should be resolved by your network's DNS server. The following restrictions apply:
	• A maximum of 10 entries is allowed.
	• Entries must be separated with a comma.
	• Do not use spaces anywhere in the list of entries.
	• Duplicate entries or entries with invalid formats are not accepted.
	Note This feature appears only if supported by your Cisco server's IOS release.

Client Settings

This window allows you to configure additional attributes for security policy such as adding or removing a backup server, Firewall Are-U-There, and Include-Local-LAN.

Note   Some of the features described below appear only if supported by your Cisco server's IOS release.

Field Reference

Table 13-11 describes the fields in this screen.

Table 13-11   Client Setting Fields

Element	Description
Backup Servers	You can specify up to ten servers by IP address or hostname as backup for the Easy VPN server, and order the list to control which servers the router will attempt to connect to first if the primary connection to the Easy VPN server fails. • **Add**—Click **Add** to specify the name or the IP address of an Easy VPN server for the router to connect to when the primary connection fails, and then enter the address or hostname in the window displayed. • **Delete**—Click **Delete** to remove a specified IP address or hostname.
Configuration Push	You can specify an Easy VPN client configuration file using a URL and version number. The Easy VPN Server sends the URL and version number to Easy VPN hardware clients requesting that information. Only Easy VPN hardware clients belonging to the group policy you are configuring can request the URL and version number you enter in this window. Enter the URL of the configuration file in the URL field. The URL should begin with an appropriate protocol, and can include usernames and passwords. The following are URL examples for downloading an upgrade file called sdm.exe: • http://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • https://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • ftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • tftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • scp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • rcp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe

Table 13-11   Client Setting Fields (continued)

Element	Description
Configuration Push	• cns:
	• xmodem:
	• ymodem:
	• null:
	• flash:sdm.exe
	• nvram:sdm.exe
	• usbtoken[0-9]:sdm.exe
	The USB token port number range is 0-9. For example, for a USB token attached to USB port 0, the URL is usbtoken0:sdm.exe.
	• usbflash[0-9]:sdm.exe
	The USB flash port number range is 0-9. For example, for a USB flash attached to USB port 0, the URL is usbflash0:sdm.exe.
	• disk[0-1]:sdm.exe
	The disk number is 0 or 1. For example, for disk number 0, the URL is disk0:sdm.exe.
	• archive:sdm.exe
	• tar:sdm.exe
	• system:sdm.exe
	In these examples, *username* is the site username and *password* is the site password.
	Enter the version number of the file in the Version field. The version number must be in the range 1 to 32767.

Table 13-11   Client Setting Fields (continued)

Element	Description
Browser Proxy	You can specify browser proxy settings for Easy VPN software clients. The Easy VPN Server sends the browser proxy settings to Easy VPN software clients requesting that information. Only Easy VPN software clients belonging to the group policy you are configuring can request the browser proxy settings you enter in this window.
	Enter the name under which the browser proxy settings were saved, or choose one of the following from the drop-down menu:
	• Choose an existing setting...
	Opens a window with a list of existing browser proxy settings.
	• Create a new setting and choose...
	Opens a window where you can create new browser proxy settings.
	• None
	Clears any browser proxy settings assigned to the group.
Firewall Are-U-There	You can restrict VPN connections to clients running Black Ice or Zone Alarm personal firewalls.
Include Local LAN	You can allow a non–split tunneling connection to access the local subnetwork at the same time as the client.
Perfect Forward Secrecy (PFS)	Enable PFS if it is required by the IPSec security association you are using.

Choose Browser Proxy Settings

From the drop-down list, choose the browser proxy settings you want to associate with the group.

Field Reference

Table 13-12 describes the fields in this screen.

Table 13-12   Choose Browser Proxy Settings

Element	Description
Proxy Settings	Choose the settings that you want to associate with the group.

Add or Edit Browser Proxy Settings

This window allows you to add or edit browser proxy settings.

Field Reference

Table 13-13 describes the fields in this screen.

Table 13-13   Browser Proxy Settings Fields

Element	Description
Browser Proxy Settings Name	If you are adding browser proxy settings, enter a name that will appear in drop-down menus listing browser proxy settings. If you are editing browser proxy settings, the name field is read-only.
Proxy Settings	Choose one of the following: • No Proxy Server You do *not* want clients in this group to use a proxy server when they use the VPN tunnel. • Automatically Detect Settings You want clients in this group to automatically detect a proxy server when they use the VPN tunnel. • Manual Proxy Configuration You want to manually configure a proxy server for clients in this group. If you choose this option, complete the procedure for manually configuring a proxy server in this help topic.

Manually Configuring a Proxy Server

If you choose Manual Proxy Configuration, follow these steps to manually configure a proxy server:

Step 1   Enter the proxy server IP address in the Server IP Address field.

Step 2   Enter the port number that proxy server uses for receiving proxy requests in the Port field.

Step 3   Enter a list of IP addresses for which you do *not* want clients to use the proxy server.

Separate the addresses with commas, and do not enter any spaces.

Step 4   If you want to prevent clients from using the proxy server for local (LAN) addresses, check the **Bypass proxy server for local address** check box.

Step 5   Click **OK** to save the browser proxy settings.

User Authentication (XAuth)

This allows you to configure additional attributes for user authentication, such as Group Lock and save Password Attributes.

Field Reference

Table 13-14 describes the fields in this screen.

Table 13-14   User Authentication (XAuth) Fields

Element	Description
XAuth Banner	Enter the text for a banner that is shown to users during XAuth requests. **Note** This feature appears only if supported by your Cisco server's IOS release.
Maximum Logins Allowed Per User	Specify the maximum number of connections a user can establish at a time. Cisco SDM supports a maximum of ten logins per user.

Table 13-14   User Authentication (XAuth) Fields (continued)

Element	Description
Group Lock	You can restrict a client to connect to the Easy VPN Server only from the specified user group.
Save Password	You can save extended authentication user name and password locally on the Easy VPN Client.

Client Update

This window allows you to set up client software or firmware update notifications, and displays existing client update entries. Existing client update entries can be selected for editing or deletion.

Notifications are sent automatically to clients which connect to the server after a new or edited client update configuration is saved. Clients already connected require manual notification. To send a manual IKE notification of update availability, choose a group policy in the group policies window and click the **Send Update** button. Group clients meeting the client update criteria are sent the notification.

> **Note** The client update window is available only if supported by your Cisco server's IOS release.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-15   Add a RADIUS Server Fields

Element	Description
Client Type	Displays the type of client for which the revision is intended.
Revisions	Displays which revisions are available.
URL Column	Displays the location of the revisions.
Add Button	Click to configure a new client update entry.
Edit Button	Click to edit the specified client update entry.
Delete Button	Click to delete the specified client update entry.

Add or Edit Client Update Entry

This window allows you to configure a new client update entry.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-16   Add a RADIUS Server Fields

Element	Description
Client Type	Enter a client type or choose one from the drop-down menu. Client type names are case sensitive.
	For software clients, the client type is usually the operating system, for example, *Windows*. For hardware clients, the client type is usually the model number, for example, *vpn3002*.
	If you are editing the client update entry, the client type is read-only.
URL	Enter the URL that leads to the latest software or firmware revision. The URL should begin with an appropriate protocol, and can include usernames and passwords.
	The following are URL examples for downloading an upgrade file called vpnclient-4-6.exe:
	• http://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• https://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• ftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• tftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• scp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• rcp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe
	• cns:
	• xmodem:
	• ymodem:
	• null:

Table 13-16   Add a RADIUS Server Fields (continued)

Element	Description
	• flash:vpnclient-4.6.exe
	• nvram:vpnclient-4.6.exe
	• usbtoken[0-9]:vpnclient-4.6.exe
	The USB token port number range is 0-9. For example, for a USB token attached to USB port 0, the URL is usbtoken0:vpnclient-4.6.exe.
	• usbflash[0-9]:vpnclient-4.6.exe
	The USB flash port number range is 0-9. For example, for a USB flash attached to USB port 0, the URL is usbflash0:vpnclient-4.6.exe.
	• disk[0-1]:vpnclient-4.6.exe
	The disk number is 0 or 1. For example, for disk number 0, the URL is disk0:vpnclient-4.6.exe.
	• archive:vpnclient-4.6.exe
	• tar:vpnclient-4.6.exe
	• system:vpnclient-4.6.exe
	In these examples, *username* is the site username and *password* is the site password.
Revisions	Enter the revision number of the latest update. You can enter multiple revision numbers by separating them with commas, for example, *4.3,4.4,4.5*. Do not use any spaces.

Cisco Tunneling Control Protocol

Cisco Tunneling Control Protocol (cTCP) enables VPN clients to operate in environments where standard ESP protocol (port 50) or IKE protocol (UDP port 500) are not permitted. For a variety of reasons, firewalls may not permit ESP or IKE traffic, thus blocking VPN communication. cTCP solves this problem by encapsulating ESP and IKE traffic in the TCP header so that firewalls do not see it.

Field Reference

Table 13-17 describes the fields in this screen.

Table 13-17   *Cisco Tunneling Control Protocol*

Element	Description
Enable cTCP	Check Enable cTCP to enable this protocol on the Easy VPN server.
Specify the port numbers	Specify the port numbers on which the Easy VPN server must listen for cTCP requests from clients, You can add a maximum of 10 port numbers. Use a comma to separate entries. Here is an example of 3 port entries: 1000,3000,4000.

Summary

This window shows you the Easy VPN Server configuration that you have created, and it allows you to save the configuration. You can review the configuration in this window and click the **Back** button to change any items.

Clicking the **Finish** button writes the information to the router running configuration. If the tunnel has been configured to operate in Auto mode, the router also attempts to contact the VPN concentrator or server.

If you want to change the Easy VPN Server configuration at a later time, you can make the changes in the Edit Easy VPN Server panel.

To save this configuration to the router running configuration and leave this wizard, click **Finish**. Changes will take effect immediately.

Table 13-18   *Summary Buttons*

Element	Description
Test VPN Connectivity After Configuring	Click to test the VPN connection you have just configured. The results of the test appear in a separate window.

Browser Proxy Settings

This window lists browser proxy settings, showing how they are configured. You can add, edit, or delete browser proxy settings. Use the group policies configuration to associate browser proxy settings with client groups.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-19   ***Add a RADIUS Server Fields***

Element	Description
Name	The name of the browser proxy settings.
Settings	Displays one of the following: • No Proxy Server No proxy server can be used by clients when they connect through the VPN tunnel. • Automatically Detect Settings Clients attempt to automatically detect a proxy server. • Manual Proxy Configuration Settings are manually configured.
Server Details	Displays the proxy server IP address and port number used.
Bypass Local Addresses	If set, prevents clients from using the proxy server for local (LAN) addresses.
Exceptions List	A list of IP addresses for which you do *not* want clients to use the proxy server.
Add Button	Configure new browser proxy settings.
Edit Button	Edit the specified browser proxy settings.
Delete Button	Delete the specified browser proxy settings. Browser proxy settings associated with one or more group policies can *not* be deleted before those associations are removed.

Editing Easy VPN Server Connections

To edit an Easy VPN Server connection, complete these steps:

Step 1   If you want to review the Cisco IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **VPN**.

Step 4   In the VPN tree, click Easy VPN Server.

Step 5   Click **Edit VPN Server**.

Step 6   Choose the VPN server connection that you want to edit.

Step 7   Click **Edit**. Then, make changes to the settings in the displayed dialogs.

Step 8   Click OK to close the dialog and send the changes to the router.

Step 9   If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it.

Edit Easy VPN Server Reference describes the configuration screens.

Edit Easy VPN Server Reference

The topics in this section describe the Edit Easy VPN Server screens:

- Edit Easy VPN Server
- Add or Edit Easy VPN Server Connection
- Restrict Access
- Group Policies Configuration
- IP Pools
- Add or Edit IP Local Pool

- Add IP Address Range

Edit Easy VPN Server

This window lets you view and manage Easy VPN server connections.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-20   *Edit Easy VPN Server Fields*

Element	Description
Add	Click **Add** to add a new Easy VPN Server.
Edit	Click **Edit** to edit an existing Easy VPN Server configuration.
Delete	Click **Delete** to delete a specified configuration.
Name	The name of the IPSec policy associated with this connection.
Interface	The name of the interface used for this connection.
Group Authorization	The name of the method list used for group policy lookup.
User Authentication Column	The name of the method list used for user authentication lookup.
Mode Configuration	Displays one of the following: • Initiate The router is configured to initiate connections with Easy VPN Remote clients. • Respond The router is configured to wait for requests from Easy VPN Remote clients before establishing connections.

Table 13-20   Edit Easy VPN Server Fields (continued)

Element	Description
Test VPN Server Button	Click to test the chosen VPN tunnel. The results of the test appear in a separate window.
Restrict Access Button	Click this button to restrict group access to the specified Easy VPN Server connection.
	This button is enabled only if both of the following conditions are met:
	• There is more than one Easy VPN Server connection using the local database for user authentication.
	• There is at least one local group policy configured.

Add or Edit Easy VPN Server Connection

This window lets you add or edit an Easy VPN Server connection.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-21   Easy VPN Server Connection Fields

Element	Description
Choose an Interface	If you are adding a connection, choose the interface to use from this list. If you are editing the connection, this list is disabled.
Choose an IPSec Policy	If you are adding a connection, choose the IPSec policy to use from this list. If you are editing the connection, this list is disabled.
Method List for Group Policy Lookup	Choose the method list to use for group policy lookup from this list. Method lists are configured by clicking **Additional Tasks** on the Cisco SDM taskbar, and then clicking the AAA node.
Enable User Authentication	Check this checkbox if you want to require users to authenticate themselves.

Table 13-21   Easy VPN Server Connection Fields (continued)

Element	Description
Method List for User Authentication	Choose the method list to use for user authentication from this list. Method lists are configured by clicking Additional tasks on the Cisco SDM taskbar, and then clicking the AAA node.
Mode Configuration	Check **Initiate** if you want the router to initiate connections with Easy VPN Remote clients.
	Check **Respond** if you want the router to wait for requests from Easy VPN Remote clients before establishing connections.

Restrict Access

This window allows you to specify which group policies are allowed to use the Easy VPN connection.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-22   Add a RADIUS Server Fields

Element	Description
Restrict Access	Click **Restrict Access** to enable restrictive access for this Easy VPN connection.
Check Boxes	Allow a group access to the Easy VPN Server connection by checking its check box. Deny a group access to the Easy VPN Server connection by unchecking its check box.

Group Policies Configuration

This window lets you view, add, clone, and choose group policies for editing or deletion. Group policies are used to identify resources for Easy VPN Remote clients.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-23   *Group Policies Configuration Fields*

Element	Description
Common Pool	Click **Common Pool** to designate an existing pool as a common pool for all group policies to use. If no local pools have been configured, this button is disabled. Pools can be configured by clicking **Additional Tasks > Local Pools**, or when you configure Easy VPN Server connections.
Add Edit Clone Delete	Use these buttons to manage group policies on the router. Clicking **Clone** displays the Group Policy edit tabs.
Send Update	Click to send an IKE notification of software or firmware updates to active clients of the chosen group. If this button is disabled, the chosen group does not have client update configured. To set up client update notifications for the chosen group, click the **Edit** button and then click the **Client Update** tab.
Group Name	The name of the group policy.
Pool	The IP address pool used by the clients in this group.
DNS	The DNS servers used by the clients in this group.
WINS	The WINS servers used by the clients in this group.
Domain Name	The domain name used by the clients in this group.
ACL	If split tunneling is specified for this group, this column may contain the name of an ACL that defines which traffic is to be encrypted.
Details Window	The Details window is a list of feature settings and their values for the chosen group policy. Feature settings are displayed only if they are supported by your Cisco router's IOS release, and apply only to the chosen group. The following feature settings may appear in the list:

Table 13-23   Group Policies Configuration Fields (continued)

Element	Description
	• Authentication—Values indicate a preshared key if one was configured, or a digital certificate if a preshared key was not configured.
	• Maximum Connections Allowed—Shows the maximum number of simultaneous connections allowed. Cisco SDM supports a maximum of 5000 simultaneous connections per group.
	• Access Restrict—Shows the outside interface to which the specified group is restricted.
	• Backup Servers—Shows the IP address of backup servers that have been configured.
	• Firewall Are-U-There—Restricts connections to devices running Black Ice or Zone Alarm firewalls.
	• Include Local LAN—Allows a connection *not* using split tunneling to access the local stub network at the same time as the client.
	• PFS (perfect forward secrecy)—PFS is required for IPSec.
	• Configuration Push, URL, and Version—The server sends a configuration file from the specified URL and with the specified version number to a client.
	• Group Lock—Clients are restricted to the group.
	• Save Password—XAuth credentials can be saved on the client.
	• Maximum Logins—The maximum number of connections a user can establish simultaneously. Cisco SDM supports a maximum of 10 simultaneous logins per user.
	• XAuth Banner—The text message shown to clients during XAuth requests.

IP Pools

This window lists the IP address pools available to group policies configured on the router. Depending upon the area of Cisco SDM you are working in, **Add**, **Edit**, and **Delete** buttons may be available, and the name of the window varies depending on the area of Cisco SDM you are working in. You can use these to manage local IP pools on the router.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-24   *IP Pools Fields*

Element	Description
Pool Name Column	The name of the IP address pool.
IP Address Range	The IP address range for the selected pool. A range of 2.2.2.0 to 2.2.2.254 provides 255 addresses.
Cache Size	The size of the cache for this pool.
Group Name	If a local pool is configured with the group option using the CLI, the name of the group is displayed in the group name column. This column is not displayed in all Cisco SDM areas.
	Note You cannot configure local pools with the group option using Cisco SDM.

Add or Edit IP Local Pool

This window lets you create or edit a local pool of IP addresses.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-25   Add or Edit IP Local Pool Fields

Element	Description
Pool Name	If you are creating a pool, enter the pool name. If you are editing a pool, this field is disabled.
IP Address Range	Enter or edit the IP address ranges for the pool in this area. A pool can contain more than one IP address range. Use the Add, Edit, and Delete buttons to create additional ranges, edit ranges, and delete IP address ranges.
Cache Size	Enter or edit the cache size for this pool in this field.

Add IP Address Range

This window lets you add an IP address range to an existing pool.

Field Reference

Table 13-6 describes the fields in this screen.

Table 13-26   Add IP Address Range Fields

Element	Description
Start IP Address	Enter the lowest IP address in the range. For example, if you are defining a range between 10.10.10.1 to 10.10.10.254, enter 10.10.10.1.
End IP Address	Enter the highest IP address in the range. For example, if you are defining a range between 10.10.10.1 to 10.10.10.254, enter 10.10.10.254.

Enhanced Easy VPN

The following sections describe the Cisco Router and Security Device Manager configuration screens for Enhanced Easy VPN.

Interface and Authentication

Specify the router interface to which the virtual template interface is to be unnumbered, and specify the method to use for authentication in this window.

Interface

A virtual template interface must be unnumbered to a router interface to obtain an IP address.

Cisco recommends that you unnumber the virtual template interface to a loopback address for greatest flexibility. To do this, click **Unnumbered to new loopback interface** and enter an IP address and subnet mask for the loopback interface. A sample loopback IP address and subnet mask is 127.0.0.1, 255.255.255.0.

To unnumber the virtual template interface to another interface, click **Unnumbered to** and choose the interface. You should choose the interface that terminates the tunnel on the router. Click **Details** to view IP address, authentication, policy, and other information about the interface that you are choosing.

Authentication

Select the method that Easy VPN clients are to use to authenticate themselves to the Easy VPN Server configured on the router. Pre-shared keys require that you communicate the key to administrators of Easy VPN clients. Digital certificates do not require this, but each client must enroll for and receive a digital certificate.

RADIUS Servers

Identify the RADIUS servers that the router will use for authorization and group policy lookup and the VPN groups configured on the RADIUS servers in the RADIUS Servers window.

Field Reference

Table 14-1 describes the fields in this screen.

Table 14-1   RADIUS Servers Fields

Element	Description
RADIUS Client Source	Configuring the RADIUS source allows you to specify the source IP address to be sent in packets bound for the RADIUS server. To view the IP address and other information about an interface, select the interface and click the **Details** button. This option can have the following values:
	• Router chooses source—Choose **Router chooses source** if you want the source IP address in the RADIUS packets to be the address of the interface through which the RADIUS packets exit the router. • Interface name—If you choose a specific router interface, the source IP address in the RADIUS packets will be the address of that interface. The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco Access Control Server (ACS) version 3.3 or later.

Table 14-1   RADIUS Servers Fields

Element	Description
	✎ **Note** Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.
RADIUS Server List	
Server IP	The Server IP column lists the IP addresses of each configured server, for example, 192.168.108.14
Parameters	The Parameters column lists the authorization and accounting ports for each server. For example, the column might contain the following entry for a RADIUS server: `Authorization Port 1645; Accounting Port 1646`
Select	The Select column contains a checkbox for each configured server. Check the box next to each server that you want to be used. The router does not contact a RADIUS server if the box next to it is not checked.
Add	Click **Add** to create an entry for a RADIUS server.
Edit	Select a server entry and click **Edit** to change the information the router has for that server.
Ping	Select a server entry and click **Ping** to test the connection between the router and the RADIUS server.

Table 14-1   RADIUS Servers Fields

Element	Description
VPN Groups in RADIUS Server	Enter the VPN groups configured on the RADIUS server that you want this connection to give access to. Use a comma to separate entries. A sample set of entries follows: `WGP-1, WGP-2, ACCTG, CSVC` These names must match the group names configured on the RADIUS server. For easy administration, they should also match the group names you configure for the easy VPN clients.
PKI-based user policy download	Check **PKI-based user policy download** if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate. This option is displayed under the following conditions: • The router runs a Cisco IOS 12.4(4)T or later image. • You choose digital certificate authentication in the IKE policy configuration. • You choose RADIUS or RADIUS and Local group authorization.

Group Authorization and Group User Policies

You can create user groups that each have their own IP address pool, client update configuration, split tunneling configuration, and other custom settings, These group attributes are downloaded to the client in that group when they connect to the Easy VPN server. The same group name must be configured on the clients who are members of the group to ensure that the correct group attributes are downloaded.

If group polices have already been configured, they appear in the list in this window, and you can select them for this connection by checking the Select box to the left of the group name.

The group name, IP address pool name, DNS and WINS server names, and domain name of each configured group is shown in the list. When you click **Add** to configure settings for a new group or click **Edit** to change settings, the changes appear in this list. To use settings for an existing group as a basis for a new group configuration, select the existing group and click **Clone**. The Add, Edit, and Clone buttons display dialogs that enable you to configure group settings.

Configure Idle Timer

Check **Configure Idle Timer** if you want to specify how long a connection is to be maintained for idle clients in the Idle Timer fields. Enter time values in HH:MM:SS format. For example, to enter 3 hours, 20 minutes, and 32 seconds, enter the following values in the fields:

```
03:20:32
```

The timeout value will apply to all groups configured for this connection.

Add or Edit Easy VPN Server: General Tab

Enter general information for the Easy VPN Server connection in this dialog.

Name for this connection

Enter a name to identify this connection the name that you enter is displayed in the Edit Easy VPN Server window.

IP Address of Virtual Tunnel Interface

Click Interface and Authentication for a description of the IP Address of Virtual Tunnel fields.

Tunnel Mode

Choose **IPSec-IPV4** in the Tunnel Mode field. The IPSec-IPV4 option enables the creation of a IP version 4 IPSec tunnel.

Description

You can enter a description that administrators in you network will find useful when changing configurations or troubleshooting the network.

Add or Edit Easy VPN Server: IKE Tab

The IKE dialog in the Add Easy VPN Server dialogs enables you to create an IKE profile for this connection.

Field Reference

xref describes the fields in this tab.

Table 14-2   *Add or Edit Easy VPN Server Connection: IKE Tab*

Element	Description
Match Identity Type	The IKE profile includes match criteria that allow the router to identify the incoming and outgoing connections to which the IKE connection parameters are to apply. Match criteria can currently be applied to VPN groups. Group is automatically chosen in the Match Identity Type field.
Add VPN groups to be associated with this IKE profile.	Build a list of groups that you want to be included in the match criteria. The groups you add are listed. • Add—Click **Add** to display a menu with the following options: – Add External Group Name—Choose **Add External Group Name** to add the name of a group that is not configured on the router, and enter the name in the dialog displayed. – Select From Local Groups—Choose **Select From Local Groups** to add the name of a group that is configured on the router. In the displayed dialog, check the box next to the group that you want to add. If all the local groups are used in other IKE profiles, SDM informs you that all groups have been selected. • Delete—Choose a group and click **Delete** to remove it from the list.

Table 14-2   Add or Edit Easy VPN Server Connection: IKE Tab

Element	Description
Mode Configuration	Choose one of the followingoptions to specify how the Easy VPN server is to handle mode configuration requests: • Respond—Choose **Respond** in the Mode Configuration field if the Easy VPN server is to respond to mode configuration requests. • Initiate—Choose **Initiate** if the Easy VPN server is to initiate mode configuration requests. • Both—Choose **Both** if the Easy VPN server is to both initiate and respond to mode configuration requests.
Group Policy Lookup Authorization Policy	Specify an authorization policy that controls access to group policy information on the AAA server. • default—Choose **default** if you want to grant access to group policy lookup information. • Policyname—To specify a policy, choose an existing policy in the list. • Add—Click **Add** to create a policy in the displayed dialog.
User Authentication Policy	Check **User Authentication Policy** if you want to allow XAuth logins, or if you want to specify a user authentication policy to use for XAuth logins. Choose one of the following options: • default—Choose **default** if you want to allow XAuth logins. • Policyname—If policies have been configured on the router, they are displayed in this list and you can select a policy to use. Click **Add** to create a policy in the displayed dialog and use it in this IKE policy.

Table 14-2   Add or Edit Easy VPN Server Connection: IKE Tab

Element	Description
Dead Peer Discovery	Click **Dead Peer Discovery** to enable the router to send dead peer detection (DPD) messages to Easy VPN Remote clients. If a client does not respond to DPD messages, the connection with it is dropped. • Keepalive Interval—Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 10 to 3600 seconds. • Retry Interval—Specify the number of seconds between retries if DPD messages fail in the Retry Interval field. The range is from 2 to 60 seconds. Dead peer discovery helps manage connections without administrator intervention, but it generates additional packets that both peers must process in order to maintain the connection.
Download user attributes from RADIUS server based on PKI certificate fields.	Check this option if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate. This option is displayed under the following conditions: • The router runs a Cisco IOS 12.4(4)T or later image. • You choose digital certificate authentication in the IKE policy configuration. • You choose RADIUS or RADIUS and Local group authorization.

Add or Edit Easy VPN Server: IPSec Tab

Enter the information to create an IPSec profile in this dialog. An IPSec profile specifies the transform sets to be used, how the Security Association (SA) lifetime is to be determined, and other information.

Transform Set Columns

Use the two columns at the top of the dialog to specify the transform sets that you want to include in the profile. The left-hand column contains the transform sets configured on the router. To add a configured tranform set to the profile, select it and click the **>>** button. If there are no tranform sets in the left-hand column, or if you need a transform set that has not been created, click **Add** and create the transform set in the displayed dialog.

Time Based IPSec SA Lifetime

Click **Time Based IPSec SA Lifetime** if you want a new SA to be established after a set period of time has elapsed. Enter the time period in the HH:MM:SS fields to the right. The range is from 0:2:0 (2 minutes) to 24:0:0 (24 hours).

Traffic Volume Based IPSec SA Lifetime

Click **Traffic Volume Based IPSec SA Lifetime** if you want a new SA to be established after a specified amount of traffic has passed through the IPSec tunnel. Enter the number of kilobytes that should pass through the tunnel before an existing SA is taken down and a new one is established. The range is from 2560 KB to 536870912 KB.

IPSec SA Idle Time

Click IPSec SA Idle Time if you want a new SA to be established after the peer has been idle for a specified amount of time. Enter the idle time period in the HH:MM:SS fields to the right. The range is from 0:1:0 (one minute) to 24:0:0 (24 hours).

Perfect Forwarding Secrecy

Click **Perfect Forwarding Secrecy** if IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this virtual template interface, or should require PFS in requests received from the peer. You can specify the following values:

- group1—The 768-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

- group2—The 1024-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

• group5—The 1536-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

Create Virtual Tunnel Interface

Enter the information for a virtual tunnel interface in this dialog.

Interface Type

Choose **default**, or **tunnel** as the interface type. If you are editing a virtual tunnel interface, the configured value is displayed and the field is read only.

Configure the interface IP address

The IP address of the virtual tunnel interface can be unnumbered to another interface, or it can have no IP address. Choose **IP Unnumbered** and choose an interface name in the Unnumbered to field, or choose **No IP address**.

Tunnel Mode

Cisco SDM currently supports the IPSec-IPv4 tunnel mode and it is selected.

Select Zone

This field appears when the router runs a Cisco IOS image that supports Zone-Policy Based Firewall (ZPF), and a zone has been configured on the router. If you want this virtual tunnel interface to be a zone member, click the button to the right of this field. Click **Select a Zone** and select the zone that you want the interface to be a member of, or click **Create a Zone** to create a new zone for this interface.

Note   It is not required that the virtual tunnel interface be a member of a zone. However, the router does not forward traffic between zone-member interfaces and non zone-member interfaces.

DMVPN

These help topics provide information about Dynamic Multipoint Virtual Private Network (DMVPN) configuration screens.

Dynamic Multipoint VPN

This wizard will help you to configure your router as a Dynamic Multipoint VPN (DMVPN) hub or DMVPN spoke. A typical VPN connection is a point-to-point IPSec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes using a GRE over IPSec tunnel. IPSec traffic is routed through the hub to the spokes in the network. Cisco SDM allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

The following link contains more information about DMVPN (requires CCO login ID).

Multipoint IPSec VPNs

Cisco SDM supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully-meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPNs and DMVPNs using crypto maps are managed and modified using the CLI. Cisco SDM supports the configuration of a DMVPN starting from IOS version 12.2(13)T.

Cisco SDM supports the configuration of a single DMVPN on a router.

In this screen, identify your router as a hub or as a spoke in the DMVPN network.

It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the SpokeConfiguration feature available in the Summary window to generate a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

Create a spoke (client) in Dynamic Multipoint VPN

Select if your router is a spoke in the DMVPN network. Spokes are the logical endpoints in the network. Before starting configuration, you should ping the hub to be sure you have connectivity to it, and have all the necessary information about the hub configuration that you need. This information is listed in Dynamic Multipoint VPN (DMVPN) Spoke Wizard.

Create a hub (server or head-end) in Dynamic Multipoint VPN

Select if your router is a hub in the DMVPN network. The hub is the logical center point in a DMVPN network, and is connected to each spoke router via a point-to-point IPSec connection. The hub can route IPSec traffic between the spoke routers in the network.

Dynamic Multipoint VPN (DMVPN) Hub Wizard

This wizard will help you configure your router as a DMVPN hub. The hub should be configured before the spokes so that you can provide the spoke administrators with the information they need to configure their spoke routers.

The application window explains what you will be configuring. After you have finished, you will need to provide spoke administrators with the following information about the hub:

- The IP address of the hub router's physical interface.
- The IP address of the hub's mGRE tunnel interface.
- The dynamic routing protocol to use to send routing updates to the DMVPN, and the autonomous system (AS) number (for EIGRP), or process ID (for OSPF) that should be used.

Cisco SDM's Configure Spoke feature enables you to create a text file that contains the information that spoke administrators need about the hub's configuration. This feature is available from the Summary window of this wizard.

You also need to tell the spoke administrators which subnet mask to use, and assign each spoke an IP address from the same subnet as the hub so that address conflicts do not occur.

Type of Hub

DMVPN networks can be configured with a single hub, or with a primary and a backup hub. Identify the type of hub you are configuring your router as.

Primary Hub

Check if the router is the primary hub in the DMVPN network.

Backup Hub

Check this button if the router is a backup hub in a full-mesh DMVPN network.

Configure Pre-Shared Key

DMVPN peers can use a pre-shared key or digital certificates to authenticate connections from each other. If pre-shared keys are used, each hub router and spoke router in the network must use the same pre-shared key.

Pre-shared keys should be exchanged with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.

Pre-Shared Key

Enter the pre-shared key used in the DMVPN network. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.

Digital Certificates

Select this button if your router uses digital certificates for authentication. Digital certificates are configured under VPN Components>Public Key Infrastructure.

Confirm Pre-Shared Key

Reenter the key for confirmation. If the values in this field and the Pre-Shared Key field do not match, Cisco SDM prompts you to reenter them.

Hub GRE Tunnel Interface Configuration

Multipoint Generic Routing Encapsulation (mGRE) is used in a DMVPN network to allow a single GRE interface on a hub to support an IPSec tunnel to each spoke router. This greatly simplifies DMVPN configuration. GRE allows routing updates to be sent over IPSec connections.

Select the interface that connects to the Internet

Select the router interface that connects to the Internet. The GRE tunnel originates from this interface.

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection. Typically, interfaces such as ISDN or Asynchronous Serial will be configured for a dialup connection.

IP Address

Enter the IP address for the mGRE interface. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254.

Subnet Mask

Enter the mask for the subnet that the GRE interfaces are in. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see IP Addresses and Subnet Masks.

Advanced Button

Cisco SDM provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings.

Advanced Configuration for the Tunnel Interface

Use this window to configure GRE tunnel parameters. Cisco SDM provides default values, but you must obtain the correct values from the hub administrator and enter them here.

The default values are provided in this help topic. If you change from the default, and need to restore it, consult this help topic.

NHRP Authentication String

Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to 8 characters long. Special characters such as spaces, question marks (?) are not allowed. All devices in the DMVPN must be configured with the same authentication string.

Cisco SDM Default: DMVPN_NW

NHRP Network ID

Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295.

Cisco SDM Default: 100000

NHRP Hold Time

Enter the number of seconds that NHRP network IDs should be advertised as valid.

Cisco SDM Default: 360

Tunnel Key

Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network.

Cisco SDM Default: 100000

Bandwidth

Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. 1000 is a typical bandwidth setting in DMVPN configurations.

Cisco SDM Default: 1000

MTU

Enter the largest amount of data, in bytes, that should be allowed in a packet travelling through the tunnel.

Cisco SDM Default: 1400

Tunnel Throughput Delay

Set a delay value for an interface, in tens of microseconds.

Cisco SDM Default: 1000

Primary Hub

If the router you are configuring is the backup hub in the DMVPN network, you need to identify the primary hub by providing its public and private IP addresses.

Public IP Address

Enter the IP address of the interface on the primary hub that is used for this tunnel. This should be a static IP address. Obtain this information from the hub administrator.

IP Address of hub's mGRE tunnel interface

Enter the IP address of the mGRE tunnel interface on the primary hub. Obtain this information from the hub administrator.

Select Routing Protocol

Use this window to specify how other networks behind your router are advertised to the other routers in the network. Select one of the following:

- EIGRP—Extended Interior Gateway Routing Protocol.
- OSPF—Open Shortest Path First.
- RIP—Routing Internet Protocol.
- Static Routing. This option is enabled when you are configuring a GRE over IPSec tunnel.

> **Note** RIP is not supported for DMVPN Hub and spoke topology but is available for DMVPN Full Mesh topology.

Routing Information

Use this window to add or edit routing information about networks behind the router that you want to advertise to the other routers in the network. The fields in this window vary according to the routing protocol specified.

For more information on RIP parameters, see Add or Edit an RIP Route.

For more information on EIGRP parameters, see Add or Edit EIGRP Route.

For more information on OSPF parameters, see Add or Edit an OSPF Route.

Please select the version of RIP to enable

Specify RIP version 1 or version 2.

Select an existing OSPF process ID/EIGRP AS number

You can select an existing process ID for OSPF or AS number for EIGRP if one has been previously configured. See Recommendations for Configuring Routing Protocols for DMVPN.

Create a new OSPF process ID/EIGRP AS number

If no process IDs exist, or if you want to use a different one, you can configure a process ID in this field.

OSPF Area ID for tunnel network

Enter a new OSPF area ID for the network. This area ID is for the tunnel network. Cisco SDM automatically adds the tunnel network to this process using this area ID.

Private networks advertised using *<protocol-name>*

This area shows the networks advertised using the selected routing protocol. If you have already configured the routing protocol you specified in this wizard, the networks that you specified to be advertised will appear in this list.

Add all the private networks that you want to advertise to the DMVPN peers using this routing process. The DMVPN wizard automatically adds the tunnel network to this process.

Network—A network address. You can enter the address of a specific network, and use the wildcard mask to generalize the advertisement.

Wild card mask—(EIGRP and OSPF protocols) A bit mask that specifies how much of the network address must match the address given in the network column. This mask can be used to have the router advertise networks in a particular range, based on the given address. A 0 bit specifies that the bit in the network address must match the corresponding bit in the given network address.

For example, if the network address were 172.55.10.3, and the wildcard mask was 0.0.255.255, the router would advertise all networks starting with the numbers 172.55, not just the network 172.55.10.3.

Area—Shown when OSPF is selected, the OSPF area number for that network. Each router in a particular OSPF area maintains a topological database for that area.

Add—Click to add a network, or a group of networks, to advertise.

Edit—Click to edit the data for an advertised network or group of networks. This button is enabled for entries that you created during the current instance of this wizard.

Delete—Click to delete the data for the selected network or group of networks. This button is enabled for entries that you created during the current instance of this wizard.

Dynamic Multipoint VPN (DMVPN) Spoke Wizard

This wizard helps you to configure your router as a spoke in a DMVPN network. Before starting the configuration, you should ping the hub to be sure that your router can send traffic to it. Also you should have all the information about the hub you need before you begin. A hub administrator who uses Cisco SDM to configure the hub can generate a text file that contains the hub information spoke administrators need.

You need to obtain the following information before you begin:

• The IP address of the hub's physical interface.

• The IP address of the hub's mGRE tunnel interface.

• The IP address and subnet mask the hub administrator tells you to use for your spoke. The hub administrator must assign addresses to each spoke to ensure that all routers in the DMVPN are in the same subnet, and that each is using a unique address.

• The routing protocol to use, and the AS number (EIGRP) or Process ID (OSPF) that is to be used to send routing updates in the DMVPN.

DMVPN Network Topology

Select the type of DMVPN network this router is a part of.

Hub and Spoke Network

Select this option if you are configuring the router in a network where each spoke router has a point-to-point GRE over IPSec connection to the DMVPN hub, and will send traffic destined for other spokes through the hub. When you select this option, the graphic displays links from the spokes to the hub.

Fully Meshed Network

Select if you are configuring the router as a spoke capable of establishing a direct IPSec tunnel to other spokes in the network. A multipoint GRE tunnel is configured on the spoke to support this functionality. When you select this option, the graphic displays links from the spokes to the hub, and links to each other.

The wizard screen list the IOS images required to support a fully-meshed DMVPN network.

Specify Hub Information

Use this window to provide necessary information about the hub in the DMVPN.

IP Address of Hub's physical interface

Enter the IP address of the interface on the hub. Obtain this address from the hub administrator. This address will be used as the tunnel destination.

IP Address of hub's mGRE tunnel interface

Enter the IP address of the mGRE tunnel interface on the hub. The mGRE tunnel addresses for the hub and spokes must be in the same subnet.

Spoke GRE Tunnel Interface Configuration

A point-to-point will be created for this spoke using the information entered in this window.

Select the interface that connects to the Internet

Select the router interface that connects to the Internet. The GRE over IPSec tunnel originates from this interface.

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected.

Re-register with hub when IP address of *interface-name* changes—This option is available when the interface you selected receives a dynamic IP address via DHCP or IPCP. Specifying' this option will allow the spoke to re-register with the hub when it receives a new IP address.

IP Address

Enter the IP address for the GRE interface to this hub. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254.

If you are configuring a spoke router, you must use the IP address assigned to your router by the hub administrator. Failure to do so may result in address conflicts.

Subnet Mask

Enter the mask for the subnet that the GRE interfaces are in. This mask must be assigned by the hub administrator and be the same for all routers in the DMVPN. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see IP Addresses and Subnet Masks.

Advanced Button

Click this button to provide NHRP and tunnel parameters for this connection.

Cisco SDM provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings. If you are configuring a spoke router, obtain the tunnel settings from the hub administrator, click this button, and enter them in the dialog box displayed.

Cisco SDM Warning: DMVPN Dependency

This window appears when the interface you have chosen for the DMVPN tunnel source has a configuration that prevents its use for DMVPN. Cisco SDM informs you of the conflict and gives you the option of allowing Cisco SDM to modify the configuration so that the conflict is removed.

Firewall

If a firewall has been applied to the interface that was designated as the tunnel source, Cisco SDM can add access rule entries to the configuration so that GRE, IPSec, and ISAKMP traffic is allowed through the firewall.

View Details

Click this button to view the access control entries that Cisco SDM will add to the access rule if you select **Allow GRE, IPSec, and ISAKMP traffic through the firewall**.

These entries allow both kinds of ISAKMP traffic, GRE traffic, Encapsulating Security Protocol (ESP), and Authentication Header Protocol (AHP).

Edit Dynamic Multipoint VPN (DMVPN)

This window displays the existing DMVPN tunnel configurations. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes. Cisco SDM supports hub-and-spoke network topology, in which GRE over IPSec traffic is routed through the hub. Cisco SDM allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

The following link contains more information about DMVPN (requires CCO login ID). Multipoint IPSec VPNs

Cisco SDM supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully-meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPNs and DMVPNs using crypto maps are managed and modified using the CLI.

Cisco SDM supports the configuration of a single DMVPN on a router.

The hub should be configured first, to establish the hub IP addresses and the routing parameters that the *spokes* must be configured with. For other recommendations on how to configure the routers in a DMVPN, see DMVPN Configuration Recommendations.

Interface

The physical interface from which this tunnel originates.

IPSec Profile

The IPSec profile that the tunnel uses. The IPSec profile defines the transform sets that are used to encrypt traffic on the tunnel. Cisco SDM supports the use of only IPSec profiles to define encryption in a DMVPN. If you want to use crypto-maps, configure the DMVPN using the CLI.

IP Address

The IP address of the GRE tunnel. The GRE tunnel is used to send routing updates to the DMVPN.

Description

A description of this tunnel.

Details panel

The Details panel shows the values for the entire configuration of the DMVPN tunnel.

Why Are some Tunnels Interfaces Shown as Read-Only?

A tunnel interface is shown as read-only if it has already been configured with crypto-map associations and NHRP parameters. You will be able to modify NHRP parameters and routing information from this window, but you must edit the IP address, tunnel source, and tunnel destination from the Interfaces and Connections window.

Add

Click to add a new DMVPN tunnel configuration.

Edit

Click to edit a selected DMVPN tunnel configuration.

Delete

Click to delete a DMVPN tunnel configuration.

General Panel

In this panel add or edit general configuration parameters of the DMVPN tunnel.

IP Address

Enter the IP address of the tunnel. This must be a private address and must be in the same subnet as the other tunnel addresses in the DMVPN. If you are configuring a spoke, you must use the address that the hub administrator has assigned to your router so that no address conflicts occur.

Mask

Enter the subnet mask that the hub administrator has assigned to the DMVPN. For more information, see IP Addresses and Subnet Masks.

Tunnel Source

Select the interface that the tunnel is to use, or enter that interface's IP address. See Using Interfaces with Dialup Configurations before you select an interface configured for a dialup connection.

Tunnel Destination

Click **This is a multipoint GRE tunnel** if this is a DMVPN tunnel in a fully-meshed network. Click **IP/Hostname** and specify an IP address or hostname if this is a hub-and-spoke network

IPSec Profile

Select a configured IPSec profile for this tunnel. The IPSec profile defines the transform sets that are used to encrypt traffic on this tunnel.

MTU

> Enter the largest amount of data, in bytes, that should be allowed in a packet traveling through the tunnel.

Bandwidth

> Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. The value 1000 is a typical bandwidth setting in DMVPN configurations.

Delay

> Set a delay value for an interface, in tens of microseconds. The value 1000 is a typical delay setting in DMVPN configurations.

Tunnel Key

> Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network.

This is a multipoint GRE Tunnel

> Check if this to be an mGRE tunnel interface, an interface capable of maintaining connections to multiple peers. If this router is being configured as a DMVPN hub, you must check this box to allow the hub to establish connections with all spokes. If the router is being configured as a spoke, check this box if you are configuring a fully meshed DMVPN. In this way, a spoke can establish a connection to the hub to send traffic and receive next hop information to directly connect to all other spokes in the DMVPN.

NHRP Panel

> Use this panel to provide NHRP configuration parameters.

Authentication String

Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to 8 characters long. All NHRP stations in the DMVPN must be configured with the same authentication string.

Hold Time

Enter the number of seconds that NHRP network IDs should be advertised as valid.

Network ID

Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295. The network ID must be unique for each NHRP station.

Next Hop Server

This area lists the IP addresses of the next hop servers that this router can contact. This area must contain the IP address of the primary and secondary hub if this is a spoke router. If this is a hub, this area must contain the IP addresses of the other hub routers in the DMVPN.

Click **Add** to enter the IP address of a next hop server. Select a server, and click **Delete** to delete it from the list.

NHRP Map

This area lists the available IP-to-NBMA address mappings. Click **Add** to create a new map. After you create the map, it will be added to this list. Click **Edit** to modify a selected map. Click **Delete** to remove a selected map configuration.

NHRP Map Configuration

Use this window to create or edit a mapping between IP and NBMA addresses.

Statically configure the IP-to-NMBA address mapping of IP destinations connected to an NBMA network.

Click this button if you are configuring a spoke in a fully meshed network. Cisco SDM treats backup hubs as spokes to primary hubs, so also click this if you are configuring a backup hub. In this part of the window you are providing the address information that the spoke or backup hub needs to contact the primary hub.

Destination Reachable through NBMA network—Enter the IP address of the mGRE tunnel configured on the primary hub. Spokes and backup hubs use this tunnel information to establish contact with the hub and create an mGRE tunnel to it. Spokes use the tunnel to send encrypted data to the hub and to query the hub for next hop information to other spokes.

NBMA Address directly reachable— Enter the static IP Address of the interface on the primary hub that supports the mGRE tunnel.

Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.

Use this area of the window to provide information used by routing protocols.

Dynamically add spokes' IP addresses to hub's multicast cache—Configure this option if you are configuring a primary or a backup hub. This option is needed by the hub to send routing updates to all connected DMVPN spokes.

IP address of NBMA address directly reachable—If you are configuring a spoke in a full meshed DMVPN, or a backup hub, check this box, and provide the static IP Address of the interface on the primary hub that supports the mGRE tunnel.

Routing Panel

Use this panel to configure routing information for the DMVPN cloud.

Routing Protocol

Select the dynamic routing protocol that the hub and spoke routers in this DMVPN use to perform routing. Note that all the routers in the DMVPN must be configured for the routing protocol that you select.

- RIP—Routing Internet Protocol
- OSPF—Open Shortest Path First

   • EIGRP—Extended Interior Gateway Routing Protocol

RIP Fields

If you selected RIP as the dynamic routing protocol, select **Version 1**, **Version 2**, or **Default**. If you select **Version 2**, the router will include the subnet mask in the routing update. If you select **Default**, the router will send out Version 2 updates, but it will be able to receive RIP Version 1 or Version 2 updates.

Turn off split horizon—If this is the hub router, check this box to turn off split horizon on the mGRE tunnel interface. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.

OSPF Fields

If you selected OSPF, the following fields must be completed:

OSPF process ID—Enter the process ID. This value identifies the OSPF process to other routers. See Recommendations for Configuring Routing Protocols for DMVPN.

OSPF Network Type—Select point-to-multipoint or broadcast. Point-to-multipoint causes OSPF to add routes to the routing table on spoke routers. If you wish to avoid this, you can select broadcast.

OSPF Priority—The OSPF priority identifies this router as a hub or as a spoke. If this is a hub router, enter a priority value of 2. If this is a spoke router, enter a priority value of 0.

EIGRP Fields

If you selected EIGRP, the following fields must be completed:

Autonomous System Number—Enter the Autonomous System Number for the group of routers using EIGRP. Routers with the same EIGRP autonomous system number maintain a topological database of routers in the region identified by that number. See Recommendations for Configuring Routing Protocols for DMVPN.

Turn off split horizon—If this is the hub router, check this box to turn on split horizon on the mGRE tunnel interface. Leave it unchecked to disable split horizon. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.

Use original next hop— If this is a DMVPN hub router, EIGRP will advertise this router as the next hop. Check this box to have EIGRP use the original IP next hop when advertising routes to the DMVPN spoke routers.

How Do I Configure a DMVPN Manually?

You can configure your router as a DMVPN hub or spoke using the VPN Components windows and the Edit Dynamic Multipoint VPN (DMVPN) window. In order to do so you need to complete the following tasks:

- Configure an IPSec profile. You cannot configure a DMVPN connection until you have configured at least one IPSec profile.
- Configure the DMVPN connection.
- Specify the networks you want to advertise to the DMVPN cloud.

Procedures for these tasks are given below:

To configure an IPSec Profile:

You need to configure an IPSec policy, and then configure a DMVPN tunnel.

Step 1   Click **VPN** in the left panel, and then click **VPN Components.**

Step 2   Click the IPSec Profiles branch, and then click **Add** in the IPSec Profiles window.

Step 3   Name the profile, and select the transform sets it is to contain in the Add an IPSec profile window. You can enter a short description if you want to.

Step 4   Click **OK**.

To configure a DMVPN connection:

Step 1   In the VPN tree, click the **Dynamic Multipoint VPN** branch.

Step 2   Click **Edit Dynamic Multipoint VPN** (**DMVPN**).

Step 3   Click **Add**.

Step 4   In the DMVPN Tunnel Configuration window, complete the General, NHRP, and Routing tabs to create a DMVPN tunnel.Consult the online help for more information about a particular field.

To specify the networks you want to advertise to the DMVPN:

If there are networks behind your router that you want to advertise to the DMVPN, you can do so by adding the network numbers in the Routing windows.

Step 1   From the left panel, click **Routing**.

Step 2   In the Routing window, select the routing protocol that you specified in DMVPN configuration, and click **Edit**.

Step 3   Add the network numbers that you want to advertise.

C H A P T E R 16

VPN Global Settings

These help topics describe the VPN Global Settings windows.

VPN Global Settings

This window displays the VPN global settings for the router.

Field Reference

Table 16-1 describes the fields in this screen.

Table 16-1   VPN Global Settings Fields

Element	Description
Edit Button	Click the **Edit** button to add or change VPN global settings.
Enable IKE	The value is True if IKE is enabled; it is False if IKE is disabled. ✎ **Note** If IKE is disabled, VPN configurations will not operate. You can click **Edit** and enable IKE in the IKE tab of the VPN Global Settings screen.
Enable Aggressive Mode	The value is True if Aggressive Mode is enabled; it is False if Aggressive Mode is disabled.The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.

Table 16-1   *VPN Global Settings Fields*

Element	Description
XAuth Timeout	The number of seconds the router is to wait for a a system to respond to the XAuth challenge.
IKE Identity	Either the host name of the router or the IP address that the router will use to identify itself in IKE negotiations.
Dead Peer Detection	Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer. If DPD is enabled, the following additional information is displayed: • IKE Keepalive (Sec)—The value is the number of seconds that the router waits between sending IKE keepalive packets. • IKE Retry (Sec)—The value is the number of seconds that the router waits between attempts to establish an IKE connection with the remote peer. By default, "2" seconds is displayed. • DPD Type—Either **On Demand** or **Periodic**. If set to **On Demand**, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If set to **Periodic**, the router sends DPD messages at the interval specified by the IKE Keepalive value.
IPSec Security Association (SA) Lifetime (Sec)	The amount of time after which IPSec security associations (SAs) will expire and be regenerated. The default is 3600 seconds (1 hour).

Table 16-1   VPN Global Settings Fields

Element	Description
IPSec Security Association (SA) Lifetime (Kilobytes)	The number of kilobytes that the router can send over the VPN connection before the IPSec SA expires. The SA will be renewed after the shortest lifetimes is reached.
Syslog Messages for Easy VPN Connections	This field can have the following values: • Enabled—Syslog messages are enabled for all Easy VPN connections. • Enabled for groups *name*, *name*—Syslog messages are enabled for the groups listed. • Disabled—Syslog messages are disabled.

VPN Global Settings: IKE

This window lets you specify global settings for IKE and IPSEC.

Enable IKE

Leave this box checked if you want to use VPN.

⚠

Caution   If IKE is disabled, VPN configurations will not work.

Enable Aggressive mode

The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.

Identity (of this router)

This field specifies the way the router will identify itself. Select either **IP address** or **host name**.

XAuth Timeout

The number of seconds the router is to wait for a response from a system requiring XAuth authentication.

Enable Dead Peer Detection (DPD)

Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer.

The Enable Dead Peer Detection checkbox is disabled when the Cisco IOS image that the router is using does not support DPD.

Keepalive

Specify the number of seconds that the router should maintain a connection when it is not being used.

Retry

Specify the number of seconds that the router should wait between attempts to establish an IKE connection with a peer. The default value is '2' seconds.

DPD Type

Select **On Demand** or **Periodic**.

If set to **On Demand**, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message.

If set to **Periodic**, the router sends DPD messages at the interval specified by the IKE Keepalive value.

VPN Global Settings: IPSec

Edit global IPSec settings in this window.

Authenticate and Generate new key after every

> Check this box and specify the time interval at which the router should authenticate and generate a new key. If you do not specify a value, the router will authenticate and generate a new key every hour.

Generate new key after the current key encrypts a volume of

> Check this box and specify the number of kilobytes that should be encrypted by the current key before the router authenticates and generates a new one. If you do not specify a value, the router will authenticate and generate a new key after the current key has encrypted 4,608,000 kilobytes.

VPN Global Settings: Easy VPN Server

Make global settings for Easy VPN server connections in this screen.

Field Reference

Table 16-2 describes the fields in this screen.

Table 16-2   *VPN Global Settings: Easy VPN Server Fields*

Element	Description
Common Pool	You can configure a common IP address pool for all clients to use. If a group does not have a specific pool, clients belonging to that group will be allocated an IP address from this common pool. Select a common pool—Select a pool name from this list. If no pools are configured, you click **Additional Tasks > Local Pools > Add**, and configure a pool in the displayed dialog. Then, return to this screen and select it.
Enable Syslog messages	Check **Enable Syslog messages** to enable Syslog messages for client connections. You can specify the scope of this option with the following options: • Enable Syslog messages for all client connections—Check this option to enable Syslog messages for all groups that connect to the Easy VPN server. • Enable Syslog messages for the following groups—Check this option to enable Syslog messages for the groups that you specify. Then, enter the group names in the box, separating one group name from another with a comma. A sample set of entries follows: `WGP-1, WGP-2, ACCTG, CSVC` The router must use Cisco IOS 12.4(4)T or later for this part of the screen to be displayed.

VPN Key Encryption Settings

The VPN Key Encryption Settings window appears if the Cisco IOS image on your router supports Type 6 encryption, also referred to as *VPN key encryption*. You can use this window to specify a master key to use when encrypting VPN keys, such as pre-shared keys, Easy VPN keys, and XAuth keys. When encrypted, these keys will not be readable by someone viewing the router's configuration file.

Enable VPN Keys Encryption

Check to enable encryption of these keys.

Current Master Key

This field contains asterisks (*) when a master key has been configured.

New Master Key

Enter a new master key in this field. Master keys must be at least 8 characters long and can be as long as 128 characters.

Confirm Master Key

Reenter the master key in this field for confirmation. If the values in this field and in the New Master Key field do not match, Cisco SDM prompts you to reenter the key.

VPN Global Settings

C H A P T E R 17

IP Security

IP Security (IPSec) is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec.

Cisco SDM lets you configure IPSec transform sets, rules, and policies.

Use the IPSec tree to go to the IPSec configuration windows that you want to use.

IPSec Policies

This window displays the IPSec policies configured on the router, and the crypto maps associated with each policy. IPSec policies are used to define VPN connections. To learn about the relationship between IPSec policies, crypto maps, and VPN connections, see More about VPN Connections and IPSec Policies.

Icon

 If this icon appears next to the IPSec policy, it is read-only, and it cannot be edited. An IPSec policy may be read-only if it contains commands that Cisco SDM does not support.

 Cisco Router and Security Device Manager 2.5 User's Guide

 17-1

  OL-4015-12

Name

The name of this IPSec policy.

Type

One of the following:

- ISAKMP—IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. Cisco SDM supports Internet Security Association and Key Management Protocol (ISAKMP) crypto maps.

- Manual—IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.

  Cisco SDM does not support the creation of manual crypto maps. Cisco SDM treats as read-only any manual crypto maps that have been created using the command-line interface (CLI).

- Dynamic—Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device.

  Cisco SDM does not support the creation of dynamic crypto maps. Cisco SDM treats as ready only any dynamic crypto maps created using the CLI.

Crypto Maps in this IPSec policy

Name

The name of the IPSec policy of which the crypto map is a part.

Seq. No.

When an IPSec policy is used in a VPN connection, the combination of the sequence number and IPSec policy name uniquely identifies the connection.

Peers

This column lists the IP addresses or host names of the peer devices specified in the crypto map. Multiple peers are separated by commas.

Transform Set

This column lists the transform sets used in the crypto map.

Dynamic Crypto Maps Sets in this IPSec Policy

Dynamic Crypto Map Set Name

The name of this dynamic crypto map set. Names enable administrators to understand how the crypto map set is used.

Sequence Number

The sequence number for this dynamic crypto map set.

Type

Type is always Dynamic.

What Do You Want to Do?

If you want to:	Do this:
Add an IPSec policy to the configuration.	Click **Add**.
Edit an existing IPSec policy.	Select the policy, and click **Edit**.
Remove a crypto map entry from a policy.	Select the policy, and click **Edit**. In the window, select the crypto map you want to remove, and click **Delete**. Then, click **OK** to return to this window.
Remove an IPSec policy.	Select the policy, and click **Delete**.

Add or Edit IPSec Policy

Use this window to add or edit an IPSec policy.

Name

The name of this IPSec policy. This name can be any set of alphanumeric characters. It may be helpful to include the peer names in the policy name, or to include other information that will be meaningful to you.

Crypto Maps in this IPSec policy

This box lists the crypto maps in this IPSec policy. The list includes the name, the sequence number, and the transform set that makes up this crypto map. You can select a crypto map and edit it or delete it from the IPSec policy.

If you want to add a crypto map, click Add. If you want Cisco SDM to guide you through the process, check **Use Add Wizard**, and then click **Add**.

Icon

If a crypto map is read-only, the read-only icon appears in this column. A crypto map may be read-only if it contains commands that Cisco SDM does not support.

Dynamic Crypto Maps Sets in this IPSec Policy

This box lists the dynamic crypto map sets in this IPSec policy. Use the **Add** button to add an existing dynamic crypto map set to the policy. Use the **Delete** button to remove a selected dynamic crypto map set from the policy.

What Do You Want to Do?

If you want to:	Do this:
Add a crypto map to this policy.	Click **Add**, and create a crypto map in the Add crypto map panels. Or, check **Use Add Wizard**, and then click **Add**. **Note** The wizard allows you to add only one transform set to the crypto map. If you need multiple transform sets in the crypto map, do not use the wizard.
Edit a crypto map in this policy.	Select the crypto map, click **Edit**, and edit the crypto map in the Edit crypto map panels.
Remove a crypto map from this policy.	Select the crypto map, and click **Delete**.

Add or Edit Crypto Map: General

Change general crypto map parameters in this window. This window contains the following fields.

Name of IPSec Policy

A read-only field that contains the name of the policy in which this crypto map is used. This field does not appear if you are using the Crypto Map Wizard.

Description

Enter or edit a description of the crypto map in this field. This description appears in the VPN Connections list, and it can be helpful in distinguishing this crypto map from others in the same IPSec policy.

Sequence Number

A number that, along with the IPSec policy name, is used to identify a connection. Cisco SDM generates a sequence number automatically. You can enter your own sequence number if you wish.

Security Association Lifetime

IPSec security associations use shared keys. These keys, and their security associations time out together. There are two lifetimes: a timed lifetime and a traffic-volume lifetime. The security association expires when the first of these lifetimes is reached.

You can use this field to specify a different security association lifetime for this crypto map than the lifetime that is specified globally. In the Kilobytes field, you can specify the lifetime in the number of kilobytes sent, up to a maximum of 4608000. In the HH:MM:SS fields, you can specify the lifetime in hours, minutes, and seconds. You can also specify both a timed and a traffic-volume lifetimes. If both are specified, the lifetime will expire when the first criterion has been satisfied.

Enable Perfect Forwarding Secrecy

When security keys are derived from previously generated keys, there is a security problem, because if one key is compromised, then the others can be compromised also. Perfect Forwarding Secrecy (PFS) guarantees that each key is derived independently. It thus ensures that if one key is compromised, no other keys will be. If you enable PFS, you can specify use of the Diffie-Hellman group1, group2, or group5 method.

Note If your router does not support group5, it will not appear in the list.

Enable Reverse Route Injection

Reverse Route Injection (RRI) is used to populate the routing table of an internal router running Open Shortest Path First (OSPF) protocol or Routing Information Protocol (RIP) for remote VPN clients or LAN-to-LAN sessions.

Reverse Route Injection dynamically adds static routes to the clients connected to the Easy VPN server.

Add or Edit Crypto Map: Peer Information

A crypto map includes the hostnames or IP addresses of the peers involved in the security association. This screen allows you to add and remove peers associated with this crypto map. Multiple peers provide the router with multiple routes for encrypted data.

If you want to:	Do this:
Add a peer to the Current List.	Enter the IP address or host name of the peer, and click **Add**.
Remove a peer from the Current List.	Select the peer, and click **Remove**.

Add or Edit Crypto Map: Transform Sets

Use this window to add and edit the transform set used in the crypto map. A crypto map includes the hostnames or IP addresses of the peers involved in the security association. Multiple peers provide the router with multiple routes for encrypted data. However, the devices at both ends of the VPN connection must use the same transform set.

Use the Crypto Map Wizard if it is sufficient for your router to offer a crypto map with one transform set.

Use **Add New Crypto Map...** with **Use Add Wizard** unchecked if you want to manually configure a crypto map with multiple transforms sets (up to six) to ensure that the router can offer one transform set that the peer it is negotiating with will accept. If you are already in the Crypto Map Wizard, exit the wizard, uncheck **Use Add Wizard**, and click **Add New Crypto Map...**.

If you manually configure a crypto map with multiple transforms sets, you can also order the transform sets. This will be the order that the router will use to negotiate which transform set to use.

Available Transform Sets

Configured transform sets available for use in crypto maps. In the Crypto Map Wizard, the available transform sets are in the **Select Transform Set** drop-down list.

If no transform sets have been configured on the router, only the default transform sets provided with Cisco SDM are shown.

Note
- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the window.

- Not all IOS images support all the transform sets that Cisco SDM supports. Transform sets unsupported by the IOS image will not appear in the window.

- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the window.

Details of Selected Transform Set (Crypto Map Wizard Only)

Shows the name, encryption, authentication characteristics, and other parameters of the chosen crypto map.

If this icon appears next to the transform set, it is read-only, and it cannot be edited.

Selected Transform Sets In Order of Preference (Manual Configuration of Crypto Map Only)

The transform sets that have been chosen for this crypto map, in the order in which they will be used. During negotiations with a peer, the router will offer transform sets in the order given in this list. You can use the up and down arrow buttons to reorder the list.

What Do You Want to Do? (Crypto Map Wizard Only)

If you want to:	Do this:
Use the selected transform set for the crypto map.	Click **Next**.
Use another existing transform set.	Select it in the Select Transform Set list, and click **Next**.
Use a new transform set.	Click **Add**, and create the transform set in the Add Transform Set window. Then, return to this window, and click **Next**.
Edit the selected transform set.	Click **Edit**, and edit the transform set in the Edit Transform Set window.
Add more transform sets to this crypto map. You may wish to do this to ensure that the router can offer a transform set that the peer will agree to use.	Leave the crypto map wizard, uncheck **Use Add Wizard**, and click **Add Crypto Map**. The Transform Set tab allows you to add and order transform sets.

What Do You Want to Do? (Manual Configuration of Crypto Map Only)

If you want to:	Do this:
Add a transform set to the Selected Transform Sets box.	Select a transform set in the Available Transform Sets box, and click the right-arrow button.
Remove a transform set from the Selected Transform Sets box.	Select the transform set you want to remove, and click the left-arrow button.
Change the preference order of the selected transform sets.	Select a transform set, and click the up button or the down button.
Add a transform set to the Available Transform Sets list.	Click **Add**, and configure the transform set in the Add Transform Set window.
Edit a transform set in the Available Transform Sets list.	Click **Edit**, and configure the transform set in the Edit Transform Set window.

Add or Edit Crypto Map: Protecting Traffic

You can configure the crypto map to protect all traffic (Crypto Map Wizard only) or choose an IPSec rule to protect specified traffic.

Protect all traffic between the following subnets (Crypto Map Wizard Only)

Use this option to specify a single source subnet (a subnet on the LAN) whose traffic you want to encrypt, and one destination subnet supported by the peer that you specified in the Peers window. All traffic flowing between other source and destination subnets will be sent unencrypted.

Source

Enter the address of the subnet whose outgoing traffic you want to protect, and specify the subnet mask. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

All traffic from this source subnet that has a destination IP address on the destination subnet will be encrypted.

Destination

Enter the address of the destination subnet, and specify the mask for that subnet. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format.

All traffic going to the hosts in this subnet will be encrypted.

IPSec Rule (Create/Select an access-list for IPSec traffic)

You can add or change the IPSec rule used in this crypto map. Use this option if you need to specify multiple sources and destinations, and/or specific types of traffic to encrypt. An IPSec rule can consist of multiple entries, each specifying different traffic types and different sources and destinations. Any packets that do not match the criteria in the IPSec rule are sent unencrypted.

Note   If you are adding an IPSec rule for a VPN connection that uses a tunnel interface, the rule must specify the same source and destination data as the tunnel configuration.

To add or change the IPSec rule for the crypto map, click the **...** button to the right of the IPSec rule field and choose one of the following:

- **Select an existing rule (ACL)**—If the rule you want to use has already been created, choose the rule, then click **OK**.

- **Create a new rule and select**—If the rule you need has not been created, create the rule, then click **OK**.

- **None**—If you want to clear a rule association. The IPSec rule field shows the name of the IPSec rule in use, but if you choose **None**, the field becomes blank.

Another way to add or change the IPSec rule for this crypto map is to enter the number of the IPSec rule directly in the IPSec rule field.

Note   IPSec rules must be extended rules, not standard rules. If the number or name you enter identifies a standard rule, Cisco SDM will display a warning message when you click OK.

Dynamic Crypto Map Sets

This window lists the dynamic crypto map sets configured on the router.

Add/Edit/Delete Buttons

Use these buttons to manage the crypto maps in the window. If you try to delete a crypto map set associated with an IPSec policy, Cisco SDM prevents you from doing so. You must disassociate the crypto map from the policy before deleting it. You can do this in the IPSec Policies window.

Name

The name of the dynamic crypto map.

Type

Always Dynamic.

Add or Edit Dynamic Crypto Map Set

Add or edit a dynamic crypto map set in this window.

Name

If you are adding a dynamic crypto map, enter the name in this field. If you are editing a crypto map set, this field is disabled, and you cannot change the name.

Crypto maps in this IPSec Policy

This area lists the crypto maps used in this set. Use the **Add**, **Edit**, and **Delete** buttons to add, remove, or modify crypto maps in this list.

Associate Crypto Map with this IPSec Policy

Sequence Number

Enter a sequence number to identify this crypto map set. This sequence number cannot be in use by any other crypto map set.

Select the Dynamic Crypto Map Set

Select the dynamic crypto map set you want to add from this list.

Crypto Maps in this Dynamic Crypto Map Set

This area lists the names, sequence numbers, and peers in the dynamic crypto map set you selected.

IPSec Profiles

This window lists configured IPSec profiles on the router. IPSec profiles consist of one or more configured transform sets; the profiles are applied to mGRE tunnels to define how tunneled traffic is encrypted.

Name

The name of the IPSec profile.

Transform Set

The transform sets used in this profile.

Description

A description of the IPSec profile.

Add

Click to add a new IPSec profile.

Edit

> Select an existing profile and click **Edit** to change the profile configuration.

Delete

> Click to edit a selected IPSec profile. If the profile you are deleting is currently used in a DMVPN tunnel, you must configure the DMVPN tunnel to use a different IPSec profile.

Details of IPSec Profile

> This area displays the configuration of the selected IPSec profile. For a description of the information displayed in this area see Add or Edit IPSec Profile.

Add or Edit IPSec Profile

> Enter the information to create an IPSec profile in this dialog. An IPSec profile specifies the transform sets to be used, how the Security Association (SA) lifetime is to be determined, and other information.

Transform Set Columns

> Use the two columns at the top of the dialog to specify the transform sets that you want to include in the profile. The left-hand column contains the transform sets configured on the router. To add a configured tranform set to the profile, select it and click the **>>** button. If there are no tranform sets in the left-hand column, or if you need a transform set that has not been created, click **Add** and create the transform set in the displayed dialog.

IKE Profile Association

> If you want to associate an IKE profile with this IPSec profile, choose an existing profile from the list. If an IKE profile has already been associated, this field is read only.

Time Based IPSec SA Lifetime

Click **Time Based IPSec SA Lifetime** if you want a new SA to be established after a set period of time has elapsed. Enter the time period in the HH:MM:SS fields to the right.

Traffic Volume Based IPSec SA Lifetime

Click **Traffic Volume Based IPSec SA Lifetime** if you want a new SA to be established after a specified amount of traffic has passed through the IPSec tunnel. Enter the number of kilobytes that should pass through the tunnel before an existing SA is taken down and a new one is established.

IPSec SA Idle Time

Click IPSec SA Idle Time if you want a new SA to be established after the peer has been idle for a specified amount of time. Enter the idle time period in the HH:MM:SS fields to the right.

Perfect Forwarding Secrecy

Click **Perfect Forwarding Secrecy** if IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this virtual template interface, or should require PFS in requests received from the peer. You can specify the following values:

- group1—The 768-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- group2—The 1024-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- group5—The 1536-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

Add or Edit IPSec Profile and Add Dynamic Crypto Map

Use this window to add or to edit an IPSec profile, or to add a dynamic crypto map.

Name

Enter a name for this profile.

Available Transform Sets

This column lists the transform sets configured on this router. To add a transform set from this list to the Selected Transform Sets column, select a transform set and click the right arrow (**>>**) button.

If you need to configure a new transform set, click the **Transform Sets** node in the IPSec tree to go to the Transform Sets window. In that window, click **Add** to create a new transform set.

Selected Transform Sets

This column lists the transform sets that you are using in this profile. You can select multiple transform sets so that the router you are configuring and the router at the other end of the tunnel can negotiate which transform set to use.

Transform Set

This screen allows you to view transform sets, add new ones, and edit or remove existing transform sets. A transform set is a particular combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can create multiple transform sets and then specify one or more of them in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry's access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When that transform set is found, it is selected and applied to the protected traffic as part of both peers' IPSec security associations.

Name

Name given to the transform set.

ESP Encryption

Cisco SDM recognizes the following ESP encryption types:

- ESP_DES—Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES supports 56-bit encryption.

- ESP_3DES—ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.

- ESP_AES_128—ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.

- ESP_AES_192—ESP, AES encryption with a 192-bit key.

- ESP_AES_256—ESP, AES encryption with a 256-bit key.

- ESP_NULL—Null encryption algorithm, but encryption transform used.

- ESP_SEAL—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.

ESP Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide both data integrity and encryption. The column will contain one of the following values:

- ESP-MD5-HMAC—Message Digest 5, Hash-based Message Authentication Code (HMAC).

- ESP-SHA-HMAC—Security Hash Algorithm, HMAC.

AH Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide data integrity but not encryption. The column will contain one of the following values:

- AH-MD5-HMAC—Message Digest 5.

- AH-SHA-HMAC—Security Hash Algorithm.

IP Compression

Indicates whether IP data compression is used.

> **Note**   If your router does not support IP compression, this box will be disabled.

Mode

This column contains one of the following values:

- Tunnel—Both the headers and data are encrypted. The mode used in VPN configurations.
- Transport—Only the data is encrypted. This mode is used when the encryption endpoints and the communication endpoints are the same.

Type

Either User Defined or Cisco SDM Default.

What Do You Want to Do?

If you want to:	Do this:
Add a new transform set to the router's configuration.	Click Add, and create the transform set in the Add Transform Set window.
Edit an existing transform set.	Select the transform set, and click **Edit**. Then edit the transform set in the Edit Transform Set window. **Note** Cisco SDM Default transform sets are read-only and cannot be edited.
Delete an existing transform set.	Select the transform set, and click **Delete**. **Note** Cisco SDM Default transform sets are read-only and cannot be deleted.

Add or Edit Transform Set

Use this window to add or edit a transform set.

To obtain a description of the allowable transform combinations, and descriptions of the transforms, click **Allowable Transform Combinations**.

Note
- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the screen.

- Not all IOS images support all the transform sets that Cisco SDM supports. Transform sets unsupported by the IOS image will not appear in the screen.

- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the screen.

- Easy VPN servers only support tunnel mode. Transport mode is not supported by Easy VPN servers.

- Easy VPN Servers only support transform sets with ESP encryption. Easy VPN servers do not support the AH algorithm.

- Easy VPN Servers do not support ESP-SEAL encryption.

Name of this transform set

This can be any name that you want. The name does not have to match the name in the transform set that the peer uses, but it may be helpful to give corresponding transform sets the same name.

Data integrity and encryption (ESP)

Check this box if you want to provide Encapsulating Security Payload (ESP) data integrity and encryption.

Integrity Algorithm

Select one of the following:

- ESP_MD5_HMAC. Message Digest 5.

- ESP_SHA_HMAC. Security Hash Algorithm.

Encryption

Cisco SDM recognizes the following ESP encryption types:

- ESP_DES. Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES supports 56-bit encryption.

- ESP_3DES. ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.

- ESP_AES_128. ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.

- ESP_AES_192. ESP, AES encryption with a 192-bit key.

- ESP_AES_256. ESP, AES encryption with a 256-bit key.

- ESP_SEAL—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.

- ESP_NULL. Null encryption algorithm, but encryption transform used.

✎

Note   The types of ESP encryption available depend on the router. Depending on the type of router you are configuring, one or more of these encryption types may not be available.

Data and address integrity without encryption (AH)

This check box and the fields below it appear if you click **Show Advanced**.

Check this box if you want the router to provide Authentication Header (AH) data and address integrity. The authentication header will not be encrypted.

Integrity Algorithm

Select one of the following:

- AH_MD5_HMAC—Message Digest 5.

- AH_SHA_HMAC—Security Hash Algorithm.

Mode

Select which parts of the traffic you want to encrypt:

- Transport. Encrypt data only—Transport mode is used when both endpoints support IPsec; this mode places the AH or ESP after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets. Transport mode should be used only when the destination of the data is always the remote VPN peer.

- Tunnel. Encrypt data and IP header—Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

IP Compression (COMP-LZS)

Check this box if you want to use data compression.

Note   Not all routers support IP compression. If your router does not support IP compression, this box is disabled.

IPSec Rules

This window shows the IPSec rules configured for this router. IPSec rules define which traffic IPSec will encrypt. The top part of the window lists the access rules defined. The bottom part shows the access rule entries for the access rule selected in the rule list.

IPSec rules contain IP address and type-of-service information. Packets that match the criteria specified in the rule are encrypted. Packets that do not match the criteria are sent unencrypted.

Name/Num

The name or number of this rule.

Used By

Which crypto maps this rule is used in.

Type

IPSec rules must specify both source and destination and must be able to specify the type of traffic the packet contains. Therefore, IPSec rules are extended rules.

Description

A textual description of the rule, if available.

Action

Either **Permit** or **Deny**. **Permit** means that packets matching the criteria in this rules are protected by encryption. **Deny** means that matching packets are sent unencrypted. For more information see Meanings of the Permit and Deny Keywords.

Source

An IP address or keyword that specifies the source of the traffic. **Any** specifies that the source can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the source IP address must match. For more information, see IP Addresses and Subnet Masks.

Destination

An IP address or keyword that specifies the destination of the traffic. **Any** specifies that the destination can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the destination IP address must match.

Service

The type of traffic that the packet must contain.

What Do You Want to Do?

If you want to:	Do this:
See the access rule entries for a particular rule.	Select the rule in the rule list. The entries for that rule appear in the lower box.
Add an IPSec rule.	Click **Add**, and create the rule in the rule window displayed.
Delete an IPSec rule.	Select the rule in the rule list, and click **Delete**.
Delete a particular rule entry.	Select the rule in the rule list, and click **Edit**. Then, delete the entry in the rule window displayed.
Apply an IPSec rule to an interface.	Apply the rule in the interface configuration window.

Internet Key Exchange

The help topics in this section describe the Internet Key Exchange (IKE) configuration screens.

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is a standard method for arranging for secure, authenticated communications. IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across the network.

Cisco SDM lets you create IKE policies that will protect the identities of peers during authentication. Cisco SDM also lets you create pre-shared keys that peers exchange.

What Do You Want to Do?

If you want to:	Do this:
Learn more about IKE.	Click **More About IKE**.
Enable IKE. You must enable IKE for VPN connections to use IKE negotiations.	Click **Global Settings**, and then click **Edit** to enable IKE and make other global settings for IKE.

If you want to:	Do this:
Create an IKE policy. Cisco SDM provides a default IKE policy, but there is no guarantee that the peer has the same policy. You should configure other IKE policies so that the router is able to offer an IKE policy that the peer can accept.	Click the **IKE Policy** node on the VPN tree. See IKE Policies for more information.
Create a pre-shared key. If IKE is used, the peers at each end must exchange a pre-shared key to authenticate each other.	Click the **Pre-Shared Key** node on the VPN tree. See IKE Pre-shared Keys for more information.
Create an IKE profile.	Click the **IKE Profile** node on the VPN tree. See IKE Profiles for more information.

IKE Policies

IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. This window shows the IKE policies configured on the router, and allows you to add, edit, or remove an IKE policy from the router's configuration. If no IKE policies have been configured on the router, this window shows the default IKE policy.

After the two peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations apply to all subsequent IKE traffic during the negotiation.

The IKE policies in this list are available to all VPN connections.

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy.

Hash

The authentication algorithm for negotiation. There are two possible values:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

Type

Either SDM_DEFAULT or User Defined. SDM_DEFAULT policies cannot be edited.

What Do You Want to Do?

If you want to:	Do this:
Learn more about IKE policies.	See **More About IKE Policies**.
Add an IKE policy to the router's configuration. Cisco SDM provides a default IKE policy, but there is no guarantee that the peer has the same policy. You should configure other IKE policies so that the router is able to offer an IKE policy that the peer can accept.	Click **Add**, and configure a new IKE policy in the Add IKE policy window.
Edit an existing IKE policy.	Choose the IKE policy that you want to edit, and click **Edit**. Then edit the IKE policy in the Edit IKE policy window. Default IKE policies are read only. They cannot be edited.
Remove an IKE policy from the router's configuration.	Choose the IKE policy that you want to remove, and click **Remove**.

Add or Edit IKE Policy

Add or edit an IKE policy in this window.

> **Note**
> - Not all routers support all encryption types. Unsupported types will not appear in the screen.
> - Not all IOS images support all the encryption types that Cisco SDM supports. Types unsupported by the IOS image will not appear in the screen.
> - If hardware encryption is turned on, only those encryption types supported by both hardware encryption and the IOS image will appear in the screen.

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy. Cisco SDM supports a variety of encryption types, listed in order of security. The more secure an encryption type, the more processing time it requires.

> **Note**
> If your router does not support an encryption type, the type will not appear in the list.

Cisco SDM supports the following types of encryption:

- Data Encryption Standard (DES)—This form of encryption supports 56-bit encryption.
- Triple Data Encryption Standard (3DES)—This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.

- AES-192—Advanced Encryption Standard (AES) encryption with a 192-bit key.
- AES-256—Advanced Encryption Standard (AES) encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. There are two options:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:

- group1—768-bit D-H Group. D-H Group 1.
- group2—1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
- group5—1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note
- If your router does not support group5, it will not appear in the list.
- Easy VPN servers do not support D-H Group 1.

Lifetime

This is the lifetime of the security association, in hours, minutes and seconds. The default is one day, or 24:00:00.

IKE Pre-shared Keys

This window allows you to view, add, edit, and remove IKE pre-shared keys in the router's configuration. A pre-shared key is exchanged with a remote peer during IKE negotiation. Both peers must be configured with the same key.

Icon

If a pre-shared key is read-only, the read-only icon appears in this column. A pre-shared key will be marked as read-only if it is configured with the **no-xauth** CLI option

Peer IP/Name

An IP address or name of a peer with whom this key is shared. If an IP address is supplied, it can specify all peers in a network or subnetwork, or just an individual host. If a name is specified, then the key is shared by only the named peer.

Network Mask

The network mask specifies how much of the peer IP address is used for the network address and how much is used for the host address. A network mask of 255.255.255.255 indicates that the peer IP address is an address for a specific host. A network mask containing zeros in the least significant bytes indicates that the peer IP address is a network or subnet address. For example a network mask of 255.255.248.0 indicates that the first 22 bits of the address are used for the network address and that the last 10 bits are for the host part of the address.

Pre-Shared Key

The pre-shared key is not readable in Cisco SDM windows. If you need to examine the pre shared key, go to **View->Running Config**. This will display the running configuration. The key is contained in the **crypto isakmp key** command.

If you want to:	Do this:
Add a pre-shared key to the router's configuration.	Click **Add**, and add the pre-shared key in the Adda new Pre Shared Key window.
Edit an existing pre-shared key.	Select the pre-shared key, and click **Edit**. Then edit the key in the Edit Pre Shared Key window.
Remove an existing pre-shared key.	Select the pre-shared key, and click **Remove**.

Add or Edit Pre Shared Key

Use this window to add or edit a pre-shared key.

Key

This is an alphanumeric string that will be exchanged with the remote peer. The same key must be configured on the remote peer. You should make this key difficult to guess. Question marks (?) and spaces must not be used in the pre-shared key.

Reenter Key

Enter the same string that you entered in the Key field, for confirmation.

Peer

Select **Hostname** if you want the key to apply to a specific host. Select **IP Address** if you want to specify a network or subnetwork, or if you want to enter the IP address of a specific host because there is no DNS server to translate host names to IP addresses

Hostname

This field appears if you selected "**Hostname**" in the Peer field. Enter the peer's host name. There must be a DNS server on the network capable of resolving the host name to an IP address.

IP Address/Subnet Mask

These fields appear if you selected "IP Address" in the Peer field. Enter the IP address of a network or subnet in the IP Address field. The pre-shared key will apply to all peers in that network or subnet. For more information, refer to IP Addresses and Subnet Masks.

Enter a subnet mask if the IP address you entered is a subnet address, and not the address of a specific host.

User Authentication [Xauth]

Check this box if site-to-site VPN peers use XAuth to authenticate themselves. If Xauth authenticationn is enabled in VPN Global Settings, it is enabled for site-to-site peers as well as for Easy VPN connections.

IKE Profiles

IKE profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPSec tunnels. An IKE profile applies parameters to an incoming IPSec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, fully qualified domain name (FQDN), and group (the virtual private network [VPN] remote client grouping).

For more information on ISAKMP profiles, and how they are configured using the Cisco IOS CLI, go to Cisco.com and follow this path:

Products and Services > Cisco IOS Software > Cisco IOS Security > Cisco IOS IPSec > Product Literature > White Papers > ISAKMP Profile Overview

IKE Profiles

The IKE Profiles area of the screen lists the configured IKE profiles and includes the profile name, the IPSec profile it is used by, and a description of the profile if one has beenprovided. If no IPSec profile uses the selected IKE profile, the value <none> appears in the Used By column.

When you create an IKE profile from this window, the profile is displayed in the list. When you use the Easy VPN server wizard to create a configuration, IKE profiles are created automatically, named by SDM, and displayed in this list.

Details of IKE Profile

The details area of the screen lists the configuration values for the selected profile. You can use it to view details without clicking the Edit button and displaying an additional dialog. If you need to make changes, click Edit and make the changes you need in the displayed dialog. To learn more about the information shown in this area, click Add or Edit an IKE Profile.

Add or Edit an IKE Profile

Enter information andmake settings in this dialog to create an IKE profile and associate it with a virtual tunnel interface.

Field Reference

Table 18-1 describes the fields in this screen.

Table 18-1   Add or Edit IKE Profile Fields

Element	Description
IKE Profile Name	Enter a name for this IKE profile. If you are editing a profile, this field is enabled.
Match Identity Type	The IKE profile includes match criteria that allow the router to identify the incoming and outgoing connections to which the IKE connection parameters are to apply. Match criteria can currently be applied to VPN groups. Group is automatically chosen in the Match Identity Type field.

Table 18-1   Add or Edit IKE Profile Fields

Element	Description

Add VPN groups to be associated with this IKE profile.	Build a list of groups that you want to be included in the match criteria. The groups you add are listed.
	
	• Add—Click **Add** to display a menu with the following options:
	
	  – Add External Group Name—Choose **Add External Group Name** to add the name of a group that is not configured on the router, and enter the name in the dialog displayed.
	
	  – Select From Local Groups—Choose **Select From Local Groups** to add the name of a group that is configured on the router. In the displayed dialog, check the box next to the group that you want to add. If all the local groups are used in other IKE profiles, SDM informs you that all groups have been selected.
	
	• Delete—Choose a group and click **Delete** to remove it from the list.

Virtual Tunnel Interface	Choose the virtual tunnel interface to which you want to associate this IKE profile from the Virtual Tunnel Interface list. If you need to create a virtual tunnel interface, click **Add** and create the interface in the displayed dialog.
Mode Configuration	Choose one of the followingoptions to specify how the Easy VPN server is to handle mode configuration requests: • Respond—Choose **Respond** in the Mode Configuration field if the Easy VPN server is to respond to mode configuration requests. • Initiate—Choose **Initiate** if the Easy VPN server is to initiate mode configuration requests. • Both—Choose **Both** if the Easy VPN server is to both initiate and respond to mode configuration requests.

Table 18-1   Add or Edit IKE Profile Fields

Element	Description
Group Policy Lookup Authorization Policy	Specify an authorization policy that controls access to group policy information on the AAA server. • default—Choose **default** if you want to grant access to group policy lookup information. • Policyname—To specify a policy, choose an existing policy in the list. • Add—Click **Add** to create a policy in the displayed dialog.
User Authentication Policy	Check **User Authentication Policy** if you want to allow XAuth logins, or if you want to specify a user authentication policy to use for XAuth logins. Choose one of the following options: • default—Choose **default** if you want to allow XAuth logins. • Policyname—If policies have been configured on the router, they are displayed in this list and you can select a policy to use. Click **Add** to create a policy in the displayed dialog and use it in this IKE policy.
Dead Peer Discovery	Click **Dead Peer Discovery** to enable the router to send dead peer detection (DPD) messages to Easy VPN Remote clients. If a client does not respond to DPD messages, the connection with it is dropped. • Keepalive Interval—Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 10 to 3600 seconds. • Retry Interval—Specify the number of seconds between retries if DPD messages fail in the Retry Interval field. The range is from 2 to 60 seconds. Dead peer discovery helps manage connections without administrator intervention, but it generates additional packets that both peers must process in order to maintain the connection.

Table 18-1   *Add or Edit IKE Profile Fields*

Element	Description
Download user attributes from RADIUS server based on PKI certificate fields.	Check this option if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate.
	This option is displayed under the following conditions:
	• The router runs a Cisco IOS 12.4(4)T or later image.
	• You choose digital certificate authentication in the IKE policy configuration.
	• You choose RADIUS or RADIUS and Local group authorization.
Description	You can add a description of the IKE profile that you are adding or editing.

Public Key Infrastructure

The Public Key Infrastructure (PKI) windows enable you to generate enrollment requests and RSA keys, and manage keys and certificates. You can use the Simple Certificate Enrollment Process (SCEP) to create an enrollment request and an RSA key pair and receive certificates online, or create an enrollment request that you can submit to a Certificate Authority (CA) server offline.

If you want to use Secure Device Provisioning (SDP) to enroll for certificates, see Secure Device Provisioning.

Certificate Wizards

This window allows you to select the type of enrollment you are performing. It also alerts you to configuration tasks that you must perform before beginning enrollment, or tasks that Cisco recommends you perform before enrolling. Completing these tasks before beginning the enrollment process helps eliminate problems that may occur.

Select the enrollment method Cisco SDM uses to generate the enrollment request.

Prerequisite Tasks

If Cisco SDM finds that there are configuration tasks that should be performed before you begin the enrollment process, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco SDM and complete the configuration. If Cisco SDM does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Simple Certificate Enrollment Protocol (SCEP)

> Click this button if you can establish a direct connection between your router and a Certificate Authority (CA) server. You must have the server's enrollment URL in order to do this. The wizard will do the following:
>
> • Gather information from you to configure a trustpoint and deliver it to the router.
>
> • Initiate an enrollment with the CA server you specified in the trustpoint.
>
> • If the CA server is available, display the CA server's fingerprint for your acceptance.
>
> • If you accept the CA server fingerprint , complete the enrollment.

Cut and Paste/Import from PC

> Click this button if your router cannot establish a direct connection to the CA server or if you want to generate an enrollment request and send it to the CA at another time. After generation, the enrollment request can be submitted to a CA at another time. Cut-and-Paste enrollment requires you to invoke the Digital Certificates wizard to generate a request, and then to reinvoke it when you have obtained the certificates for the CA server and for the router.

> **Note** Cisco SDM supports only base-64-encoded PKCS#10-type cut and paste enrollment. Cisco SDM does not support importing PEM and PKCS#12 type certificate enrollments.

Launch the selected task button

> Click to begin the wizard for the type of enrollment that you selected. If Cisco SDM has detected a required task that must be performed before enrollment can begin, this button is disabled. Once the task is completed, the button is enabled.

Welcome to the SCEP Wizard

> This screen indicates that you are using the SCEP wizard. If you do not want to use the Simple Certificate Enrollment Process, click **Cancel** to leave this wizard.

After the wizard completes and the commands are delivered to the router, Cisco SDM attempts to contact the CA server. If the CA server is contacted, Cisco SDM displays a message window with the server's digital certificate.

Certificate Authority (CA) Information

Provide information to identify the CA server in this window. Also specify a challenge password that will be sent along with the request.

> **Note** The information you enter in this screen is used to generate a trustpoint. The trustpoint is generated with a default revocation check method of CRL. If you are editing an existing trustpoint with the SCEP wizard, and a revocation method different from CRL, such as OCSP, already exists under the trustpoint, Cisco SDM will not modify it. If you need to change the revocation method, go to Router Certificates window, select the trustpoint you configured, and click the **Check Revocation** button.

CA server nickname

The CA server nickname is an identifier for the trustpoint you are configuring. Enter a name that will help you identify one trustpoint from another.

Enrollment URL

If you are completing an SCEP enrollment, you must enter the enrollment URL for the CA server in this field. For example,

```
http://CAuthority/enrollment
```

The URL must begin with the characters http://. Be sure there is connectivity between the router and the CA server before beginning the enrollment process.

This field does not appear if you are completing a cut-and-paste enrollment.

Challenge Password and Confirm Challenge Password

A challenge Password can be sent to the CA for you to use if you ever need to revoke the certificate. It is recommended that you do so, as some CA servers do not issue certificates if the challenge Password is blank. If you want to use a

challenge Password, enter that password and then reenter it in the confirm field. The challenge Password will be sent along with the enrollment request. For security purposes, the challenge password is encrypted in the router configuration file, so you should record the password and save it in a location you will remember.

This password is also referred to as a challenge password.

Advanced Options Button

Advanced options allow you to provide more information to enable the router to contact the CA server.

Advanced Options

Use this window to provide more information to enable the router to contact the CA server.

Source the certificate request from a specific interface

Check this box if you want to specify a particular interface as the source of the certificate.

HTTP Proxy and HTTP Port

If the enrollment request will be sent through a proxy server, enter the proxy server IP address, and the port number to use for proxy requests in these fields.

Certificate Subject Name Attributes

Specify the optional information that you want to be included in the certificate. Any information that you specify be included in the certificate request will be placed in the certificate, and be viewable by any party to whom the router sends the certificate.

Include router's fully qualified Domain Name (FQDN) in the certificate.

It is recommended that the router's fully qualified domain name be included in the certificate. Check this box if you want Cisco SDM to include the router's fully qualified domain name in the certificate request.

> **Note** If the Cisco IOS image running on the router does not support this feature, this box is disabled.

FQDN

If you enabled this field, enter the routers FQDN in this field. An example of an FQDN is

```
sjrtr.mycompany.net
```

Include router's IP Address

Check if you want to include a valid IP address configured on your router in the certificate request. If you check this box, you can manually enter an IP address, or you can select the interface whose IP address you want to be used.

IP Address

Click if you want to enter an IP address, and enter an IP address configured on the router in the field that appears. Enter an IP address that has been configured on the router or an address that has been assigned to the router.

Interface

Select a router interface whose IP address you want to be included in the certificate request.

Include router's serial number

Check this box if you want the serial number of the router included in the certificate.

Other Subject Attributes

The information you enter in this window will be placed in the enrollment request. CAs use the X.500 standard to store and maintain information for digital certificates. All fields are optional, but it is recommended that you enter as much information as possible.

Common Name (cn)

Enter the common name to be included in this certificate. This would be the name used to search for the certificate in the X.500 directory.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, Development, or Engineering might be organizational units

Organization (o)

Enter the organization or company name. This is the X.500 organizational name.

State (st)

Enter the state or province in which the router or the organization is located.

Country (c)

Enter the country in which the router or the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Note If the Cisco IOS image running on the router does not support this attribute, this field is disabled.

RSA Keys

You must include an RSA public key in the enrollment request. Once the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data sent to the router. The private key is kept on the router and used to decrypt the data sent by peers, and also used to digitally sign transactions when negotiating with peers.

Generate new key pair(s)

Click this button if you want to generate a new key to use in the certificate. When you generate a key pair, you must specify the modulus to determine the size of the key. This new key appears in the RSA Keys window when the wizard is completed.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Generate separate key pairs for encryption and signature

By default, Cisco SDM creates a general purpose key pair that is used for both encryption and signature. If you want Cisco SDM to generate separate key pairs for encrypting and signing documents, check this box. Cisco SDM will generate usage keys for encryption and signature.

Use existing RSA key pair

Click this button if you want to use an existing key pair, and select the key from the drop-down list.

Save to USB Token

Check the **Save keys and certificates to secure USB token** checkbox if you want to save the RSA keys and certificates to a USB token connected to your router. This checkbox appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

Summary

This window summarizes the information that you provided. The information that you provided is used to configure a trustpoint on the router and begin the enrollment process. If you enabled **Preview commands before delivering to router** in the Preferences dialog, you will be able to preview the CLI that is delivered to the router.

If you are performing an SCEP enrollment

After the commands are delivered to the router, Cisco SDM attempts to contact the CA server. If the CA server is contacted, Cisco SDM displays a message window with the server's digital certificate.

If you are performing a cut-and-paste enrollment

After the commands are delivered to the router, Cisco SDM generates an enrollment request and displays it in another window. You must save this enrollment request and present it to the CA server administrator in order to obtain the CA server's certificate, and the certificate for the router. The enrollment request is in Base64 encoded PKCS#10 format.

After you obtain the certificates from the CA server, you must restart the Cut and Paste wizard, and select **Continue an unfinished enrollment** to import the certificates to your router.

CA Server Certificate

Cisco SDM displays the digital fingerprint of the CA server's certificate. If you wish to continue the enrollment process, you must accept this certificate. If you do not accept the certificate, the enrollment does not proceed

CA server's certificate's finger print is:

Cisco SDM displays the hexadecimal value of the CA server's certificate in large type. For example:

E55725EC A389E81E 28C4BE48 12B905ACD

To accept the CA server's certificate and continue the enrollment process

Click **Yes, I accept this certificate** and then click **Next**.

To decline the CA server's certificate and stop the enrollment process

Click No, I do not accept this certificate and click **Next**.

Enrollment Status

This window informs you of the status of the enrollment process. If errors are encountered during the process, Cisco SDM displays the information it has about the error.

When status has been reported, click **Finish**.

Cut and Paste Wizard Welcome

The Cut and Paste wizard lets you generate an enrollment request and save it to your PC so that you can send it to the Certificate Authority offline. Because you cannot complete the enrollment in a single session, this wizard completes when you generate the trustpoint and the enrollment request and save it to your PC.

After you have submitted the enrollment request to the CA server manually, and received the CA server certificate and the certificate for your router, you must start the Cut and Paste wizard again to complete the enrollment and import the certificates to the router.

Enrollment Task

Specify whether you are beginning a new enrollment or you are resuming an enrollment with an enrollment request that you saved to the PC.

Begin New Enrollment

Click **Begin new enrollment** to generate a trustpoint, an RSA key pair and an enrollment request that you can save to your PC and send to the CA server. The wizard completes after you save the enrollment request. To complete the enrollment after you have receive the CA server certificate and the certificate for your router, re-enter the Cut and Paste wizard and select **Continue with an unfinished enrollment**.

Continue with an unfinished enrollment

Click this button to resume an enrollment process. You can import certificates you have received from the CA server, and you can generate a new enrollment request for a trustpoint if you need to.

Enrollment Request

This window displays the base-64-encoded PKCS#10-type enrollment request that the router has generated. Save the enrollment request to the PC. Then, send it to the CA to obtain your certificate.

Save:

Browse for the directory on the PC that you want to save the enrollment request text file in, enter a name for the file, and click **Save**.

Continue with Unfinished Enrollment

If you are continuing with an unfinished enrollment you need to select the trustpoint associated with the unfinished enrollment, and then specify the part of the enrollment process you need to complete. If you are importing a CA server certificate or a router certificate, the certificate must be available on your PC.

Select CA server nickname (trustpoint)

Select the trustpoint associated with the enrollment you are completing.

Import CA and router certificate(s)

Choose this option if you want to import both the CA server's certificate and the router's certificate in the same session. Both certificates must be available on the PC.

This option is disabled if the CA certificate has already been imported.

Import CA certificate

Choose this option to import a CA server certificate that you have saved on your PC. After you import the certificate, Cisco SDM will display the certificate's digital fingerprint. You can then verify the certificate and accept or reject it.

This option is disabled if the CA certificate has already been imported.

Import router certificate(s)

Choose this option to import a certificate for your router saved on your PC. After you import the router certificate, Cisco SDM will report on the status of the enrollment process.

> **Note**   You must import the CA server's certificate before you import the router's certificate.

Generate enrollment request

Choose this option if you need to generate an enrollment request for the selected trustpoint. The router will generate an enrollment request that you can save to the PC and send to the CA.

Cisco SDM generates a base-64 encoded PKCS#10 enrollment request.

Import CA certificate

If you have the CA server certificate on your hard disk, you can browse for it and import it to your router in this window. You can also copy and paste the certificate text into the text area of this window.

Browse Button

Click to locate the certificate file on the PC.

Import Router Certificate(s)

If you have one or more certificates for your router granted by the CA on your hard disk, you can browse for it and import it to your router.

Import more certificates

If you generated separate RSA key pairs for encryption and signature, you receive two certificates for the router. Use this button when you have more than one router certificate to import.

Remove certificate

Click the tab for the certificate you need to remove and click **Remove** certificate.

Browse

Browse to locate the certificate and import it to the router.

Digital Certificates

This window allows you to view information about the digital certificates configured on the router.

Trustpoints

This area displays summary information for the trustpoints configured on the router and allows you to view details about the trustpoints, edit trustpoints, and determine if a trustpoint has been revoked.

Details Button

The Trustpoints list only displays the name, enrollment URL, and enrollment type for a trustpoint. Click to view all the information for the selected trustpoint.

Edit Button

A trustpoint can be edited if it is an SCEP trustpoint, and if the CA server's certificate and the router's certificate have not both been successfully imported. If the trustpoint is not an SCEP trustpoint, or if both the CA server and router certificate associated with an SCEP trustpoint have been delivered, this button is disabled.

Delete Button

Click to delete the selected trustpoint. Deleting a trustpoint destroys all certificates received from the associated certificate authority.

Check Revocation Button

Click to check whether the selected certificate has been revoked. Cisco SDM displays a dialog in which you select the method to use to check for revocation. See Revocation Check and Revocation Check, CRL Only for more information.

Name	Trustpoint name.

CA Server	The name or IP address of the CA server.
Enrollment Type	One of the following:
	• SCEP—Simple Certificate Enrollment Protocol. The enrollment accomplished by connecting directly to the CA server
	• Cut and Paste—Enrollment request was imported from PC.
	• TFTP—Enrollment request was made using a TFTP server.

Certificate chain for trustpoint *name*

This area shows details about the certificates associated with the selected trustpoint.

Details Button

Click to view the selected certificate.

Refresh Button

Click to refresh the Certificate chain area when you select a different trustpoint in the Trustpoints list.

Type	One of the following:
	• RA KeyEncipher Certificate—Rivest Adelman encryption certific
	• RA Signature Certificate—Rivest Adelman signature certificate.
	• CA Certificate—The certificate of the CA organization.
	• Certificate—The certificate of the router.
Usage	One of the following:
	• General Purpose—A general purpose certificate that the router us authenticate itself to remote peers.
	• Signature—CA certificates are signature certificates.
Serial Number	The serial number of the certificate
Issuer	The name of the CA that issued the certificate.

Status	One of the following:
	• Available—The certificate is available for use.
	• Pending—The certificate has bee applied for, but is not available
Expires (Days)	The number of days the certificate can be used before it expires.
Expiry Date	The date on which the certificate expires.

Trustpoint Information

The Trustpoints list in the Router Certificates window displays the key information about each trustpoint on the router. This window displays all the information provided to create the trustpoint.

Certificate Details

This window displays trustpoint details that are not displayed in the Certificates window.

Revocation Check

Specify how the router is to check whether a certificate has been revoked in this window.

Revocation Check

Configure how the router is to check for revocations, and order them by preference. The router can use multiple methods.

Use/Method/Move Up/Move Down

Check the methods that you want to use, and use the **Move Up** and **Move Down** buttons to place the methods in the order you want to use them.

- OCSP—Contact an Online Certificate Status Protocol server to determine the status of a certificate.

- CRL—Certificate revocation is checked using a certificate revocation list.

- None—Do not perform a revocation check.

CRL Query URL

Enabled when CRL is selected. Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

OCSP URL

Enabled when OCSP is selected. Enter the URL of the OCSP server that you want to contact.

Revocation Check, CRL Only

Specify how the router is to check whether a certificate has been revoked in this window.

Verification

One of the following:

- None—Check the Certificate Revocation List (CRL) distribution point embedded in the certificate.
- Best Effort—Download the CRL from the CRL server if it is available. If it is not available, the certificate will be accepted.
- Optional—Check the CRL only if it has already been downloaded to the cache as a result of manual loading.

CRL Query URL

Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

RSA Keys Window

RSA keys provide an electronic encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adelman. The RSA system is the most commonly used encryption and authentication algorithm, and is included as a part of Cisco IOS. To use the RSA system, a network host

generates a pair of keys. One is called the *public key*, and the other is called the *private key*. The Public key is given to anyone who wants to send encrypted data to the host. The Private key is never shared. When a remote hosts wants to send data, it encrypts it with the public key shared by the local host. The local host decrypts sent data using the private key.

RSA keys configured on your router

Name	The key name. Key names are automatically assigned by Cisco SDM. The "HTTPS_SS_CERT_KEYPAIR" and "HTTPS_SS_CERT_KEYPAIR.serve shown as Read-Only. Similarly, any key that is locked/encrypted on the ro displayed with icons that indicate their status.
Usage	Either General Purpose or Usage. General purpose keys are used to encrypt sign the certificate. If separate keys are configured to encrypt data and to s certificates, these keys are labelled Usage keys.
Exportable	If this column contains a checkmark the key can be exported to another ro becomes necessary for that router to assume the role of the local router.

Key Data

Click to view a selected RSA key.

Save Key to PC Button

Click to save the data of the selected key to your PC.

Generate RSA Key Pair

Use this window to generate a new RSA key pair.

Label

Enter the label of the key in this field.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The larger the modulus size, the more secure the key is. However keys with larger modulus sizes take longer to generate and longer to process when exchanged.

Type

Select the type of key to generate, **General Purpose**, or **Usage**. General purpose keys are used for both encryption and signing of certificates. If you generate Usage keys, one set of keys will be used for encryption, and a separate set will be used for certificate signing.

Key is exportable checkbox

Check if you want the key to be exportable. An exportable key pair can be sent to a remote router if it is necessary for that router to take over the functions of the local router.

Save to USB Token

Check the **Save keys to secure USB token** checkbox if you want to save the RSA keys to a USB token connected to your router. This checkbox appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

USB Token Credentials

This window appears when you add or delete credentials, such as an RSA key pair or digital certificates, that have been saved on a USB token. For the deletion to take place, you must provide the USB token name and PIN.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN
needed to log in to the chosen USB token in **PIN**.

USB Tokens

This window allows you to configure USB token logins. This window also
displays a list of configured USB token logins. When a USB token is connected
to your Cisco router, Cisco SDM uses the matching login to log in to the token.

Add

Click **Add** to add a new USB token login.

Edit

Click **Edit** to edit an existing USB token login. Specifiy the login to edit by
choosing it in the list.

Delete

Click **Delete** to delete an existing USB token login. Specifiy the login to delete by
choosing it in the list.

Token Name

Displays the name used to log in to the USB token.

User PIN

Displays the PIN used to log in to the USB token.

Maximum PIN Retries

Displays the maximum number of times Cisco SDM will attempt to log in to the
USB token with the given PIN. If Cisco SDM is unsuccessful after trying for the
number specified, it will stop trying to log in to the USB token.

Removal Timeout

Displays the maximum number of seconds that Cisco SDM will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router.

If Removal Timeout is empty, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Displays the configuration file that Cisco SDM attempts to find on the USB token. The configuration file can be a CCCD file or a .cfg file.

CCCD refers to a boot configuration file. On USB tokens, a CCCD file is loaded using TMS software.

Add or Edit USB Token

This window allows you to add or edit USB token logins.

Token Name

If you are adding a USB token login, enter the USB token name. The name you enter must match the name of the token that you want to log in to.

A token name is set by the manufacturer. For example, USB tokens manufactured by Aladdin Knowledge Systems are named eToken.

You can also use the name "usbtoken$x$", where x is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

If you are editing a USB token login, the Token Name field cannot be changed.

Current PIN

If you are adding a USB token login, or if you are editing a USB token login that has no PIN, the Current PIN field displays <None>. If you are editing a USB token login which has a PIN, the Current PIN field displays ******.

Enter New PIN

Enter a new PIN for the USB token. The new PIN must be at least 4 digits long and must match the name of the token you want to log in to. If you are editing a USB token login, the current PIN will be replaced by the new PIN.

Reenter New PIN

Reenter the new PIN to confirm it.

Maximum PIN Retries

Choose the maximum number of times Cisco SDM will attempt to log in to the USB token with the given PIN. If Cisco SDM is unsuccessful after trying for the number specified, it will stop trying to log in to the USB token.

Removal Timeout

Enter the maximum number of seconds that Cisco SDM will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router. The number of seconds must be in the range 0 to 480.

If you do not enter a number, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Specify a configuration file that exists on the USB token. The file can be a partial or complete configuration file. The file extension must .cfg.

If Cisco SDM can log in to the USB token, it will merge the specified configuration file with the router's running configuration.

Open Firewall

This screen is displayed when Cisco SDM detects firewall(s) on interfaces that would block return traffic that the router needs to receive. Two situations in which it might appear are when a firewall will block DNS traffic or PKI traffic and prevent the router from receiving this traffic from the servers. Cisco SDM can modify these firewalls so that the servers can communicate with the router.

Modify Firewall

This area lists the exit interfaces and ACL names, and allows you to select which firewalls that you want Cisco SDM to modify. Select the firewalls that you want Cisco SDM to modify in the Action column. Cisco SDM will modify them to allow SCEP or DNS traffic from the server to the router.

Note the following for SCEP traffic:

- Cisco SDM will not modify firewall for CRL/OCSP servers if these are not explicitly configured on the router. To permit communication with CRL/OCSP servers, obtain the correct information from the CA server administrator and modify the firewallsusing the Edit Firewall Policy/ACL window.

- Cisco SDM assumes that the traffic sent from the CA server to the router will enter through the same interfaces through which traffic from the router to the CA server was sent. If you think that the return traffic from CA server will enter the router through a different interface than the one Cisco SDM lists, you need to open the firewall using the Edit Firewall Policy/ACL window. This may occur if asymmetric routing is used, whereby traffic from the router to the CA server exits the router through one interface and return traffic enters the router through a different interface.

- Cisco SDM determines the exit interfaces of the router the moment the passthrough ACE is added. If a dynamic routing protocol is used to learn routes to the CA server and if a route changes—the exit interface changes for SCEP traffic destined for the CA server—you must explicitly add a passthrough ACE for those interfaces using the Edit Firewall Policy/ACL window.

- Cisco SDM adds passthrough ACEs for SCEP traffic. It does not add passthrough ACEs for revocation traffic such as CRL traffic and OCSP traffic. You must explicitly add passthrough ACEs for this traffic using the Edit Firewall Policy/ACL window.

Details Button

Click this button to view the access control entry that Cisco SDM would add to the firewall if you allow the modification.

Open Firewall Details

This window displays the access control entry (ACE) that Cisco SDM would add to a firewall to enable various types of traffic to reach the router. This entry is not added unless you check **Modify** in the Open Firewall window and complete the wizard.

Open Firewall

Certificate Authority Server

You can configure a Cisco IOS router to serve as a Certificate Authority (CA) server. A CA server handles certificate enrollment requests from clients, and can issue and revoke digital certificates.

To create, back up, restore, or edit a CA server, go to **Configure > VPN > Public Key Infrastructure > Certificate Authority > Create CA Server**.

To manage certificates on an existing CA server, go to **Configure > VPN > Public Key Infrastructure > Certificate Authority > Manage CA Server**.

To monitor a CA server, go to **Monitor > VPN Status > CA Server**.

Create CA Server

This window allows you to launch a wizard for creating a Certificate Authority (CA) server, or a wizard for restoring a CA server. Only one CA server can be set up on a Cisco IOS router.

The CA server should be used to issue certificates to hosts on the private network so that they can use the certificates to authenticate themselves to other

Prerequisite Tasks

If Cisco SDM finds that there are configuration tasks that should be performed before you begin configuring the CA server, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco SDM

and complete the configuration. If Cisco SDM does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Create Certificate Authority (CA) Server

Click this button to create a CA server on the router. Because only one CA server can be configured on the router, this button is disabled if a CA server is already configured.

> **Note**   The CA server you configure using SDM allows you to grant and revoke certificates. Although the router does store the serial numbers and other identifying information about the certificates that it grants, it does not store the certificates themselves. The CA server should be configured with a URL to a Registration Authority (RA) server that can store certificates that the CA server grants.

Restore Certificate Authority (CA) Server

If a CA server already operates on the router, you can restore the CA server configuration, and the information. If no CA server is configured on the router, this option is disabled.

Prerequisite Tasks for PKI Configurations

Before you begin a certificate enrollment or CA server configuration, it may be necessary for you to complete supporting configuration tasks first. SDM reviews the running configuration before allowing you to begin, alerts you to configurations you must complete, and provides links that take you to the areas of SDM that allow you to complete these configurations.

SDM may generate alerts about the following configuration tasks:

- SSH credentials not verified—Cisco SDM requires you to provide your SSH credentials before beginning.

- NTP not configured—The router must have accurate time for certificate enrollment to work. Identifying a Network Time Protocol server from which your router can obtain accurate time provides a time source that is not

affected if the router needs to be rebooted. If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at the following URL:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

- DNS not configured—Specifying DNS servers helps ensure that the router is able to contact the certificate server. DNS configuration is required to contact the CA server and any other server related to certificate enrollment such as OCSP servers or CRL repositories if those servers are entered as names and not as IP addresses.

- Domain and/or Hostname not configured—It is recommended that you configure a domain and hostname before beginning enrollment.

CA Server Wizard: Welcome

The Certificate Authority (CA) server wizard guides you through the configuration of a CA server. Be sure to have the following information before you begin:

- General information about the CA server—The name that you intend to give the server, the certificate issuer name that you want to use, and the username and password that enrollees will be required to enter when sending an enrollment request to the server.

- More detailed information about the server—Whether the server will operate in Registration Authority (RA) mode or Certificate Authority (CA) mode, the level of information about each certificate that the server will store, whether the server should grant certificates automatically, and the lifetimes of the certificates granted, and open enrollment requests.

- Supporting information—Links to the RA server that will store the certificates and to the Certificate Revocation List Distribution Point (CDP) server.

CA Server Wizard: Certificate Authority Information

Enter basic information about the CA server that you are configuring in this window.

CA Server Name

Provide a name to identify the server in the CA Server Name field. This could be the host name of the router, or another name that you enter.

Grant

Choose **Manual** if you want to grant certificates manually. Choose **Auto** if you want the server to grant certificates automatically. Auto, used mostly for debug purposes, is not recommended since it will issue certificates to any requester without requiring enrollment information.

Warning   **Do not set Grant to Auto if your router is connected to the Internet. Grant should be set to Auto only for internal purposes such as when executing debugging procedures.**

CDP URL

Enter the URL to a Certificate Revocation List Distribution Point (CDP) server in the CDP URL field. The URL must be an HTTP URL. A sample URL follows:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

The Certificate Revocation List (CRL) is the list of revoked certificates. Devices needing to check the validity of another device's certificate will fetch the CRL from the CA server. Since many devices may attempt to fetch the CRL, offloading it to a remote device, preferably an HTTP server, will reduce the performance impact on the Cisco IOS router hosting the CA server. If the checking device cannot connect to the CDP, as a backup it will use SCEP to fetch the CRL from the CA server.

Issuer Name Attributes

Common Name (cn)

Enter the common name that you want to use for the certificate. This might be the CA server name, the router hostname or another name you choose.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, IT support, or Engineering might be organizational units.

Organization (o)

Enter the organization or company name.

State (st)

Enter the state or province in which the organization is located.

Country (c)

Enter the country in which the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Advanced Options

Click this button to enter advanced options for the CA server.

Advanced Options

The Advanced Options screen allows you to change default values for server settings and to specify the URL for the database that is to contain the certificate information.

Database

Configure the database level, the database URL, and database format in this section of the dialog.

Database Level

Choose the type of data that will be stored in the certificate enrollment database:

- **minimal—**Enough information is stored to continue issuing new certificates without conflict. This is the default.

- **names—**In addition to the information given by the minimal option, this includes the serial number and subject name of each certificate.

- **complete—**In addition to the information given by the minimal and names options, each issued certificate is written to the database.

Database URL

Enter the location to which the CA server will write certificate enrollment data. If no location is given, certificate enrollment data will be written to flash memory by default.

For example, to write certificate enrollment data to a tftp server, enter tftp://mytftp. To reset the database URL to flash memory, enter nvram.

Database Archive

Choose **pem** to create the archive in pem format, or **pkcs12** to create the archive in pkcs12 format.

Database Username

Enter a username for the database archive in the Database Username field. The username and password will be used to authenticate the server to the database.

Database Password and Confirm Password

Enter a password in the Database Password field, and reenter it in the Confirm Password field.

Lifetimes

Set the lifetime, or time before expiration, of items associated with the CA server. To set the lifetime for a specific item, choose it from the Lifetime drop-down list and enter a value in the Lifetime field.

You can set lifetimes for the following items:

- **Certificate**—Certificates issued by the CA server. Lifetime is entered in days, in the range 1–1825. If no value is entered, a certificate expires after one year. If a new value is entered, it affects certificates created only after that value is in effect.

- **CRL**—The Certificate Revocation List for certificates issued by the CA server. Lifetime is entered in hours, in the range 1–336. If no value is entered, a CRL expires after 168 hours (one week).

- **Enrollment-Request**—Open certificate requests existing in the enrollment database, but not including requests received through SCEP. Lifetime is entered in hours, in the range 1–1000. If no value is entered, an open enrollment request expires after 168 hours (one week).

CA Server Wizard: RSA Keys

The CA server uses public and private RSA keys to encrypt data and to sign certificates. SDM automatically generates a new key pair and gives it the name of the CA server. You can change the key modulus and type, and you can make the key exportable. You must enter a passphrase to use when restoring the CA server.

Label

This field is read-only. SDM uses the name of the CA server as the name of the key pair.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Type

By default, Cisco SDM creates a general purpose key pair that is used for both encryption and signature. If you want Cisco SDM to generate separate key pairs for encrypting and signing documents, choose **Usage Keys**. Cisco SDM will generate usage keys for encryption and signature.

Key is exportable

Check **Key is exportable** if you want the CA server key to be exportable.

Passphrase and Confirm Passphrase

In the Passphrase field, enter a passphrase to use when restoring the CA server from backup. Reenter the same passphrase in the Confirm Passphrase field.

Open Firewall

The Open Firewall window appears when a firewall configuration must be modified in order to allow communication between the CDP server and the CA server. Select the interface, and check the **Modify** box to allow SDM to modify the firewall to allow this traffic. Click **Details** to view the ACE that would be added to the firewall.

CA Server Wizard: Summary

The Summary window displays the information that you entered in the wizard screens so that you can review the information before sending it to the router. A sample summary display follows:

```
-------------------------------------------------------------
CA Server Configuration
-------------------------------------------------------------
CA Server Name :CASvr-a
Grant:Manual
CDP URL:http://192.27.108.92/snrs.com
Common Name (cn):CS1841
Organization Unit (ou):IT Support
Organization (o):Acme Enterprises
State (st):CA
Country (c):US


-------------------------------------------------------------
Advanced CA Server Configuration
-------------------------------------------------------------
Database URL:nvram:
Database Archive:pem
Database Username:bjones
Database Password:*********


-------------------------------------------------------------
RSA Keys:
-------------------------------------------------------------
```

```
CA Server will automatically generate RSA key pair with following
defaults:-
Modulus:1024
Type of Key:General Purpose
Exportable Key:No
Passphrase configured:******


------------------------------------------------------------
Firewall Pass-through ACEs for Interface(s):
------------------------------------------------------------

FastEthernet0/0
    permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

The summary display contains four sections, the CA Server Configuration section, the CA Server Advanced Configuration section, the RSA Keys section, and the Firewall Pass-through section. The name of this CA server is CAsvr-a. Certificates will be manually granted. Certificate information will be stored in nvram, in PEM format. SDM will generate a general-purpose key pair with the default modulus 1024. The key will not be exportable. an ACE will be configured to allow traffic to between the router and the CDP host with the IP address 192.27.108.92.

Manage CA Server

You can start and stop the CA server from this window, grant and reject certificate requests, and revoke certificates. If you need to change the CA server configuration, you can uninstall the server from this window and return to the Create CA Server window to create the server configuration that you need.

Name

Displays the name of the server. The name of the server was created when the server was created.

Status Icon

If the CA server is running, the word Running and a green icon is displayed. If the CA server is not running, the word Stopped and a red icon is displayed.

Start Server

The Start Server button is displayed if the server is stopped. Click **Start Server** to start the CA server.

Stop Server

The Stop Server button is displayed if the server the server is running, click **Stop Server** if you need to stop the CA server.

Backup Server

Click **Backup Server** to backup the server configuration information onto the PC. Enter the backup location in the displayed dialog.

Uninstall Server

Click to uninstall the CA server from your Cisco IOS router. All of the CA server configuration and data will be removed. If you backed up the CA server before uninstalling it, you can restore its data only after you create a new CA server. See Create CA Server.

Details of CA Server

The Details of CA Server table provides a snapshot of the CA Server configuration. The following table shows sample information.

Item Name	Item Value
CA Certificate Lifetime	1095 days
CDP URL	http://192.168.7.5
CRL Lifetime	168 hours
Certificate Lifetime	365 days
Database Level	minimal
Database URL	nvram:
Enrollment Request Lifetime	168 hours
Grant	manual

Item Name	Item Value
Issuer Name	CN=CertSvr
Mode	Certificate Authority
Name	CertSvr

See CA Server Wizard: Certificate Authority Information and Advanced Options for descriptions of these items.

Backup CA Server

You can back up the files that contain the information for the CA server to your PC. The Backup CA Server window lists the files that will be backed up. The listed files must be present in the router NVRAM for the backup to be successful.

Click **Browse** and specify a folder on the PC to which the CA server files should be backed up.

Manage CA Server Restore Window

If you have backed up and uninstalled a CA server, you can restore the server configuration to the router by clicking the **Restore CA Server** button. You must be able to provide the CA server name, complete database URL, and the backup passphrase that was used during initial configuration. When you restore the CA server, you are given the opportunity to change configuration settings.

Restore CA Server

If you have backed up the configuration for a CA server that was uninstalled, you can restore it by providing the information about it in the Restore CA Server window. You can edit settings for the server by clicking **Edit CA server settings before restoration**. You must provide the name, file format, URL to the database, and passphrase in order to back up the server or edit server settings.

CA Server Name

Enter the name of the CA server that you backed up.

File Format

Choose the file format that was specified in server configuration, either PEM or PKCS12.

Complete URL

Enter the router database URL that was provided when the CA server was configured. This is the location to which the CA server writes certificate enrollment data. Two sample URLs follow:

```
nvram:/mycs_06.p12
tftp://192.168.3.2/mycs_06.pem
```

Passphrase

Enter the passphrase that was entered when the CA server was configured.

Copy CA Server Files from PC

Check the **Copy CA Server Files from PC checkbox** if you want to copy the server information that you backed up to the PC to router nvram.

Edit CA Server settings before restoration

Click **Edit CA Server settings before restoration** if you want to change CA server configuration settings before restoring the server. See CA Server Wizard: Certificate Authority Information and CA Server Wizard: RSA Keys for information about the settings that you can change.

Edit CA Server Settings: General Tab

Edit general CA server configuration settings in this window. You cannot change the name of the CA server. For information on the settings that you can change, see CA Server Wizard: Certificate Authority Information.

Edit CA Server Settings: Advanced Tab

You can change any of the advanced CA server settings in this window. For information on these settings, see Advanced Options.

Manage CA Server: CA Server Not Configured

This window appears when you click **Manage CA Server** but no CA server is configured. Click **Create CA Server** and complete the wizard to configure a CA server on your router.

Manage Certificates

Clicking **VPN > Public Key Infrastructure > Certificate Authority > Manage Certificates** displays the Pending Requests tab and the Revoked Certificates tab. To go to the help topics for these tabs, click the following links:

- Pending Requests
- Revoked Certificates

Pending Requests

This window displays a list of certificate enrollment requests received by the CA server from clients. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

You can choose a certificate enrollment request in the list, then choose to issue (accept), reject, or delete it. The actions available depend on the status of the chosen certificate enrollment request.

Select All

Click **Select All** to select all outstanding certificate requests. When all certificate requests are selected, clicking **Grant** grants all requests. Clicking **Reject** when all certificate requests are selected rejects all the requests..

Grant

Click **Grant** to issue the certificate to the requesting client.

> **Note** The CA server windows do not show the IDs of the certificates that are granted. In case it is ever necessary to revoke a certificate, you should obtain the certificate ID from the administrator of the client that the certificate was issued for. The client administrator can determine the certificate ID by entering the Cisco IOS command sh crypto pki cert.

Delete

Click **Delete** to remove the certificate enrollment request from the database.

Reject

Click **Reject** to deny the certificate enrollment request.

Refresh

Click **Refresh** to update the certificate enrollment requests list with the latest changes.

Certificate Enrollment Requests Area

The certificate enrollment requests area has the following columns:

Request ID—A unique number assigned to the certificate enrollment request.

Status—The current status of the certificate enrollment request. The status can be Pending (no decision), Granted (issued certificate), Rejected (denied request).

Fingerprint—A unique digital client identifier.

Subject Name—The subject name in the enrollment request.

A sample enrollment request follows:

Request ID	State	Fingerprint	Subject Name
1	pending	serialNumber=FTX0850Z0GT+ hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FDBBB5E8B A

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

Revoked Certificates

This window displays a list of issued and revoked certificates. Only issued certificates can be revoked. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

The list of certificates has the following columns:

- **Certificate Serial Number**—A unique number assigned to the certificate. This number is displayed in hexadecimal format. For example, the decimal serial number 1 is displayed as 0x01.

- **Revocation Date**—The time and date that the certificate was revoked. If a certificate was revoked at 41 minutes and 20 seconds after midnight on February 6, 2007, the revocation date is displayed as 00:41:20 UTC Feb 6 2007.

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

> **Note**   The certificate ID does not always match the request ID shown in the CA server
> windows. It may be necessary to obtain the ID of the certificate to be revoked from
> the administrator of the client for which the certificate was granted. See Pending
> Requests for information on how the client administrator can determine the
> certificate ID.

Revoke Certificate

You can revoke certificates that have been granted by this CA server in this
window.

Certificate ID

Enter the ID of the certificate that you are revoking.

> **Note**   The certificate ID does not always match the request ID shown in the CA server
> windows. It may be necessary to obtain the ID of the certificate to be revoked from
> the administrator of the client for which the certificate was granted. See Pending
> Requests for information on how the client administrator can determine the
> certificate ID.

Cisco IOS SSL VPN

Cisco IOS SSL VPN provides Secure Socket Layer (SSL) VPN remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. This enables companies to extend their secure enterprise networks to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS SSL VPN also enables access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hotspots, where an IT department cannot easily deploy and manage the VPN client software necessary for IPsec VPN connections.

There are three modes of SSL VPN access: clientless, thin-client and full-tunnel client. Cisco SDM supports all three. Each mode is described below:

- **Clientless SSL VPN**—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to use within a web browser, such as intranet access, and online tools that employ a web interface.

- **Thin Client SSL VPN** (port-forwarding Java applet)—Thin Client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as POP3, SMTP, IMAP, Telnet, and SSH.

- **Full Tunnel Client SSL VPN**—Full tunnel client mode offers extensive application support through its dynamically downloaded SSL VPN client software for Cisco IOS SSL VPN. With the Full tunnel Client for Cisco IOS SSL VPN, we delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that allows network layer connectivity access to virtually any application.

Cisco IOS SSL VPN Contexts, Gateways, and Policies describes how the components of a Cisco IOS SSL VPN configuration work together.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

This chapter contains the following sections:

- Cisco IOS SSL VPN links on Cisco.com
- Creating an SSL VPN Connection
- Editing SSL VPN Connections
- Additional Help Topics

Cisco IOS SSL VPN links on Cisco.com

This help topic lists the current links that provide the most useful information on Cisco IOS SSL VPN.

The following link provides access to documents that describe Cisco IOS SSL VPN. Return to this link from time to time for the latest information.

www.cisco.com/go/iosSSLVPN

The following link explains how to configure a AAA server using the RADIUS protocol for Cisco IOS SSL VPN.

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Creating an SSL VPN Connection

To create an SSL VPN connection, complete the following tasks:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   On the Cisco SDM toolbar, click **Configure**.

Step 3   On the Cisco SDM category bar, click **VPN**.

Step 4   In the VPN tree, choose **SSL VPN**.

Step 5   In the Create SSL VPN tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco SDM either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 6   Choose the task you want to complete. If you are creating the first SSL VPN connection, choose **Create a new SSL VPN**.

Step 7   Click **Launch the selected task** to begin configuring the connection.

Step 8   Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 9   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 10   If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **OK** to send the configuration to the router, or click **Cancel** to discard it. If you did not make this setting, clicking Finish sends the configuration to the router.

Create an SSL VPN Connection Reference describes the screens that you use to complete this task.

Create an SSL VPN Connection Reference

The topics in this section describe the Create SSL VPN screens.

- Create SSL VPN
- Persistent Self-Signed Certificate
- Welcome
- SSL VPN Gateways
- User Authentication

- Configure Intranet Websites
- Add or Edit URL
- Customize SSL VPN Portal
- SSL VPN Passthrough Configuration
- User Policy
- Details of SSL VPN Group Policy: Policyname
- Select the SSL VPN User Group
- Select Advanced Features
- Thin Client (Port Forwarding)
- Add or Edit a Server
- Full Tunnel
- Locating the Install Bundle for Cisco SDM
- Enable Cisco Secure Desktop
- Common Internet File System
- Enable Clientless Citrix
- Summary

Create SSL VPN

You can use Cisco IOS SSL VPN wizards to create a new Cisco IOS SSL VPN or to add new policies or features to an existing Cisco IOS SSL VPN.

Click Cisco IOS SSL VPN to get an overview of the features that Cisco SDM supports. Cisco IOS SSL VPN Contexts, Gateways, and Policies describes how the components of a Cisco IOS SSL VPN configuration work together.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

Prerequisite Tasks

AAA and certificates must be configured on the router before you can begin a Cisco IOS SSL VPN configuration. If either or both of these configurations are missing, a notification appears in this area of the window, and a link is provided

that enables you to complete the missing configuration. When all prerequisite configurations are complete, you can return to this window and start configuring Cisco IOS SSL VPN.

Cisco SDM enables AAA without user input. Cisco SDM can help you generate public and private keys for the router, and enroll them with a certification authority to obtain digital certificates. See Public Key Infrastructure for more information. Alternatively, you can configure a persistent self-signed certificate that does not require approval by a CA. For more information on the persistent self-signed certificate feature, see the information at this link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_gui de09186a008040adf0.html#wp1066623

Make sure that the entire URL is present in the link field in your browser.

Create a new SSL VPN

Select this option to create a new Cisco IOS SSL VPN configuration. This wizard enables you to create a Cisco IOS SSL VPN with one user policy and a limited set of features. After you complete this wizard, you can use the other wizards to configure addition policies and features for the Cisco IOS SSL VPN. You can return to this wizard to create additional Cisco IOS SSL VPN configurations.

When you use Cisco SDM to create the first Cisco IOS SSL VPN configuration on a router, you create a Cisco IOS SSL VPN context, configure a gateway, and create a group policy. After you complete the wizard, click **Edit SSL VPN** to view the configuration and familiarize yourself with how Cisco IOS SSL VPN components work together. For information that will help you understand what you see, click Cisco IOS SSL VPN Contexts, Gateways, and Policies.

Add a new policy to an existing SSL VPN for a new group of users

Select this option to add a new policy to an existing Cisco IOS SSL VPN configuration for a new group of users. Multiple policies allow you to define separate sets of capabilities for different groups of users. For example, you might define a policy for engineering, and a separate policy for sales.

Configure advanced features for an existing SSL VPN

Select this option to configure additional features for an existing Cisco IOS SSL VPN policy. You must specify the context under which this policy is configured.

Launch the selected task button

> Click to begin the configuration that you selected. You will receive a warning message if you cannot complete the task that you chose. If there is a prerequisite task that you need to complete, you will be told what it is and how to complete it.

Persistent Self-Signed Certificate

> You can provide the information for a persistent self-signed certificate in this dialog. Using the information that you provide, the HTTPS server will generate a certificate that will be used in the SSL handshake. Persistent self-signed certificates remain in the configuration even if the router is reloaded, and are presented during the SSL handshake process. New users must manually accept these certificates, but users who have previously done so do not have to accept them again if the router was reloaded.
>
> For more information on the persistent self-signed certificate feature, see the information at this link:
>
> http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623
>
> Make sure that the entire URL is present in the link field in your browser.

Name

> Cisco SDM places the name Router_Certificate in this field. You can change the name if you want to do so. This corresponds to the subject name that would be used in a certificate request.

Length of RSA Key

> Cisco SDM places the value 512 in this field. You can specify a longer key, such as 1024, if you want to do so. The key length should be a multiple of 64.

Subject

> Provide the information for the fields in the subject area. For more information on these fields, see the information in Other Subject Attributes.

Generate Button

After providing the information in this window, click **Generate** to have the router create the persistent self-signed certificate.

Welcome

The Welcome window for each wizard lists the tasks that the wizard enables you to complete. Use this information to ensure that you are using the correct wizard. If you are not, click **Cancel** to return to the Create SSL VPN window and choose the wizard that you want to use.

When you provide all the information asked for by the wizard, the Summary window displays the information that you provided. To see the Cisco IOS CLI commands that you are delivering to the router, click **Cancel** to leave the wizard, and go to **Edit** > **Preferences**, and check **Preview commands before delivering to router.** Then restart the wizard and provide the information that it asks for. When you deliver the configuration to the router, an additional window is displayed that allows you to view the Cisco IOS CLI commands you are delivering.

SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides the IP address and the digital certificate for the SSL VPN contexts that use it. You can provide the information for a gateway in this window, and the information that will allow users to access a portal.

IP Address and Name Fields

Use these fields to create the URL that users will enter to access the Cisco IOS SSL VPN portal. The IP address list contains the IP addresses of all configured router interfaces, and all existing Cisco IOS SSL VPN gateways. You can use the IP address of a router interface if it is a public address that the intended clients can reach, or you can use another public IP address that the clients can reach.

If you use an IP address that has not already been used for a gateway, you create a new gateway.

Allow Cisco SDM access through *IP Address* Checkbox

Check if you want to continue to access Cisco SDM from this IP address. This checkbox appears if you entered the IP address you are currently using to access Cisco SDM.

Note If you check this checkbox, the URL that you must use to access Cisco SDM changes after you deliver the configuration to the router. Review the information area at the bottom of the window to learn which URL to use. Cisco SDM places a shortcut to this URL on the desktop of your PC that you can use to access Cisco SDM in the future.

Digital certificate

If you are creating a new gateway, select the digital certificate that you want the router to present to clients when they log in to the gateway. If you chose the IP address of an existing gateway, the router will use the digital certificate configured for that gateway, and this field is disabled.

Information area

When you provide the information in the IP Address and Name fields, this area contains the URL that users will enter. You must provide this URL to the users for whom you are creating this Cisco IOS SSL VPN.

If you checked **Allow Cisco SDM access through *IP address***, the URL that you must use in the future to access Cisco SDM is shown in this area. Cisco SDM places a shortcut to this URL on the desktop of your PC after you deliver the Cisco IOS SSL VPN configuration to the router.

User Authentication

Use this window to specify how the router is to perform user authentication. The router can authenticate Cisco IOS SSL VPN users locally, or it can send authentication requests to remote AAA servers.

External AAA server Button

Click if you want the router to use an AAA server to authenticate Cisco IOS SSL VPN users. The router will use the AAA servers that are listed in this window. If there are no AAA servers configured, you can configure them in this window. To use this option, there must be at least one AAA server configured on the router.

Locally on this router Button

Click if you want the router to authenticate users itself. The router will authenticate each user displayed in this window. If no users are configured on the router, you can add users in this window.

First on an external AAA server and then locally on this router Button

Click if you want the router to authenticate using a AAA server first, and if authentication fails, to attempt local authentication. If the user is not configured on either a configured AAA server or locally on the router, authentication for that user fails.

Use the AAA authentication method list Button

Click if you want the router to use a method list for authentication. A method list contains the authentication methods that should be used. The router attempts the first authentication method in the list. If authentication fails, the router tries the next method in the list and continues until the user is authenticated, or until it reaches the end of the list.

AAA servers configured for this router List

This list contains the AAA servers that the router uses to authenticate users. If you choose to authenticate users with AAA servers, this list must contain the name or IP address of at least one server. Use the **Add** button to add information for a new server. To manage AAA configurations on the router, leave the wizard, click **Additional Tasks**, and then click the AAA node in the Additional Tasks tree. This list does not appear if you have chosen **Locally on this router**.

Create user accounts locally on this router

Enter the users that you want the router to authenticate in this list. Use the **Add and Edit** buttons to manage the users on the router. This list does not appear if you chose **External AAA server**.

Configure Intranet Websites

Configure groups of intranet websites that you want users to have access to in this window. These links will appear in the portal that the users of this Cisco IOS SSL VPN see when they log in.

Action and URL List Columns

If you are adding a policy to an existing Cisco IOS SSL VPN context, there may be URL lists present in the table that is displayed. Check **Select** if you want to use a displayed URL list for the policy.

To create a new list, click **Add** and provide the required information in the dialog displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this table.

Add or Edit URL

Add or edit the information for a Cisco IOS SSL VPN link in this window.

Label

The label appears in the portal that is displayed when users log in to the Cisco IOS SSL VPN. For example, might use the label Payroll calendar if you are providing a link to the calendar showing paid holidays and paydays.

URL Link

Enter or edit the URL to the corporate intranet website that you want to allow users to visit.

Customize SSL VPN Portal

The settings that you make in this screen determine the appearance of the portal to the user. You can select among the predefined themes listed, and obtain a preview of the portal as it would appear if that theme were used.

Theme

Select the name of a predefined theme.

Preview

This area shows what the portal looks like with the selected theme. You may want to preview several themes to determine which one you want to use.

SSL VPN Passthrough Configuration

In order for users to be able to connect to the intranet, access control entries (ACE) must be added to firewall and Network Access Control (NAC) configurations to permit SSL traffic to reach the intranet. Cisco SDM can configure these ACE for you, or you can configure them yourself by going to **Firewall and ACL > Edit Firewall Policy/ACL** and making the necessary edits.

If you are working in the Cisco IOS SSL VPN wizard, click **Allow SSL VPN to work with NAC and Firewall** if you want Cisco SDM to configure these ACEs. Click **View Details** to view the ACEs that Cisco SDM would create. An entry that Cisco SDM adds might look like this example:

```
permit tcp any host 172.16.5.5 eq 443
```

If you are editing a Cisco IOS SSL VPN context, Cisco SDM displays the affected interface and ACL that is applied to it. Click **Modify** to allow Cisco SDM to add entries to the ACL to allow SSL traffic to pass through the firewall. Click **Details** to view the entry that Cisco SDM adds. The entry will be one similar to the one already shown.

User Policy

This window allows you to choose an existing Cisco IOS SSL VPN and add a new policy to it. For example, you might have created a Cisco IOS SSL VPN named Corporate, and you want to define intranet access for a new group of users that you name Engineering.

Select existing SSL VPN

Choose the Cisco IOS SSL VPN for which you want to create a new group of users. The policies already configured for that Cisco IOS SSL VPN are displayed in a box under the list. You can click any of them to display the details of the policy. See Details of SSL VPN Group Policy: Policyname for more information.

Name of new policy

Enter the name that you want to give the new group of users. The area below this field lists the group policies that already exist for this Cisco IOS SSL VPN.

Details of SSL VPN Group Policy: Policyname

This window displays the details of an existing Cisco IOS SSL VPN policy.

Services

This area lists the services, such as URL mangling, and Cisco Secure Desktop, that this policy is configured for.

URLs exposed to users

This area lists the intranet URLs exposed to users who are governed by this policy.

Servers exposed to users

This area displays the IP addresses of the port forwarding servers that this policy is configured to use.

WINS servers

This area displays the IP addresses of the WINS servers that this policy is configured to use.

Select the SSL VPN User Group

Choose the Cisco IOS SSL VPN and associated user group for which you want to configure advanced services in this window.

SSL VPN

Choose the Cisco IOS SSL VPN that the user group is associated with from this list.

User Group

Choose the user group for which you will configure advanced features. The contents of this list is based on the Cisco IOS SSL VPN that you chose.

Select Advanced Features

Choose the features that you want to configure in this window. The wizard will display windows that allow you to configure the features that you choose.

For example, if you click Thin Client (Port Forwarding), Cisco Secure Desktop, and Common Internet File System (CIFS), the wizard will display configuration windows for these features.

You must choose at least one feature to configure.

Thin Client (Port Forwarding)

Remote workstations must sometimes run client applications to be able to communicate with intranet servers. For example Internet Mail Access Protocol (IMAP) or Simple Mail Transfer Protocol (SMTP) servers may require workstations to run client applications in order to send and receive e-mail. The Thin-Client feature, also known as port forwarding, allows a small applet to be downloaded along with the portal so that a remote workstation can communicate with the intranet server.

This window contains a list of the servers and port numbers configured for the intranet. Use the **Add** button to add a server IP address and port number. Use the **Edit** and **Delete** buttons to make changes to the information in this list and to remove information for a server.

The list that you build appears in the portal that clients see when they log in.

Add or Edit a Server

Add or edit server information in this window.

Server IP Address

Enter the IP address or hostname of the server.

Server port on which service is listening

Enter the port the server is listening on for this service. This may be a standard port number for the service, such as port number 23 for Telnet, or it may be a nonstandard port number for which a Port-to-Application Map (PAM) has been created. For example if you changed the Telnet port number on the server to 2323, and you created a PAM entry for that port on that server, you would enter 2323 in this window.

Port on Client PC

Cisco SDM enters a number in this field, beginning with the number 3000. Each time you add an entry, Cisco SDM increments the number by 1. Use the entries that Cisco SDM has placed in this field.

Description

Enter a description for the entry. For example, if you are adding an entry that enables users to telnet to a server at 10.10.11.2, you could enter "Telnet to 10.10.11.2." The description you enter appears on the portal.

Learn More

Click this link for more information. You can view that information now by clicking Learn More about Port Forwarding Servers.

Full Tunnel

Full tunnel clients must download the full tunnel software and obtain an IP address from the router. Use this window to configure the IP address pool that full tunnel clients will draw from when they log in and to specify the location of the full tunnel install bundle.

> **Note**   If the software install bundle is not already installed, there must be sufficient memory in router flash for Cisco SDM to install it after you complete this wizard.

Enable Full Tunnel Checkbox

Check to allow the router to download the full tunnel client software to the user's PC, and to enable the other fields in this window.

IP Address Pool

Specify the IP address pool that full tunnel clients will draw from. You can enter the name of an existing pool in the field, or you can click the button to the right of the field and choose **Select an existing IP pool** to browse the list of pools, Choose **Create a new pool** and complete the dialog that is displayed to create a new pool. The address pool that you choose or create must contain addresses in the corporate intranet.

Keep the Full Tunnel Client software installed on client's PC Checkbox

Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this checkbox, clients download the software each time they establish communication with the gateway.

Install Full Tunnel Client Checkbox

Check if you want to install the full tunnel client software at this time. You can also install the client software when editing this Cisco IOS SSL VPN.

The full tunnel client software must be installed on the router so that clients can download it to establish full-tunnel connectivity. If the Full Tunnel software was installed along with Cisco SDM, the path to it automatically appears in the Location field, as shown in Example 21-1.

Example 21-1   Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```

In Example 21-1, the Full Tunnel install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with disk*n* or slot*n*.

If this field is empty, you must locate the install bundle so that Cisco SDM can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking on the Download latest... link at the bottom of the window. This link takes you to the following web page:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Note   You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle for Cisco SDM to learn how to locate the Full Tunnel software install bundle, and supply a path to it for Cisco SDM to use.

Advanced Button

Click to configure advanced options such as split tunneling, split DNS, and client Microsoft Internet Explorer settings.

Locating the Install Bundle for Cisco SDM

Use the following procedure to locate software install bundles for Cisco SDM so that it can use that location in the Cisco IOS SSL VPN configuration, or, if necessary, load the software onto the router.

Note   You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Step 1   Look at the **Location** field. If the path to the install bundle is in that field, no further action need be taken. Cisco SDM configures the router to download the software from that location. Example 21-2 shows a path to a software install bundle.

Example 21-2   Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```

Step 2   If the Location field is empty, click the **...** button to the right of the field to specify the location of the software.

Step 3   If the software is installed on the router, choose **Router File System** and then browse for the file.

If the software is on your PC, choose **My Computer** and browse for the file.

Cisco SDM places the router file system or PC path you specified in the Location field.

Step 4   If the software is not on the router or on your PC, you must download it to your PC, and then provide the path to the file in this field.

   a.   Click the Download latest... link in the window. You are connected to the download page for the software you want.

   b.   There may be software packages available for Cisco IOS platforms and other platforms on the web page that appears. Double-click the latest version of the software that you want to download for Cisco IOS platforms, and provide your CCO username and password when prompted to do so.

   c.   Download the package to the PC.

   d.   In the Cisco IOS SSL VPN wizard, click the **...** button to the right of the Location field, choose **My Computer** in the Select Location window that is displayed, and navigate to the directory in which you placed the file.

   e.   Select the install bundle file then click **OK** in the Select Location window. Cisco SDM places that path in the Location field. examples shows an install bundle located on the PC's desktop.

Example 21-3   Full Tunnel Package Installed on Router

```
C:\Documents and Settings\username\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco SDM installs the software onto the router from the PC directory that you specified when you deliver the configuration to the router by clicking **Finish**.

Enable Cisco Secure Desktop

The router can install Cisco Secure Desktop on the user PC when the user logs in to the Cisco IOS SSL VPN. Web transactions can leave cookies, browser history files, e-mail attachments, and other files on the PC after the user logs out. Cisco Secure Desktop create a secure partition on the desktop and uses a Department of Defense algorithm to remove the files after the session terminates.

Install Cisco Secure Desktop

Clients must download the Cisco Secure Desktop software install bundle from the router. If this software was installed along with Cisco SDM, the path to it automatically appears in the **Location** field as shown in Example 21-4.

Example 21-4   Cisco Secure Desktop Package Installed on Router

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

In Example 21-4, the Cisco Secure Desktop install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with disk*n* or slot*n*.

If this field is empty, you must locate the install bundle so that Cisco SDM can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking the **Download latest...** link at the bottom of the window. This link takes you to the following web page:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Note   You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle for Cisco SDM to learn how to locate the Cisco
Secure Desktop software install bundle, and supply a path to it for Cisco Cisco
SDM to use.

Common Internet File System

Common Internet File System (CIFS) allows clients to remotely browse, access,
and create files on Microsoft Windows-based file servers using a web browser
interface.

WINS Servers

Microsoft Windows Internet Naming Service (WINS) servers maintain the
database that maps client IP addresses to their corresponding NetBIOS names.
Enter the IP addresses of the WINS servers in your network in this box. Use
semicolons (;) to separate addresses.

For example, to enter the IP addresses 10.0.0.18 and 10.10.10.2, you enter
10.0.0.18;10.10.10.2 in this box.

Permissions

Specify the permissions to grant to users.

Enable Clientless Citrix

Clientless Citrix allows users to run applications such as Microsoft Word or Excel
on remote servers in the same way that they would run them locally, without the
need for client software on the PC. The Citrix software must be installed on one
or more servers on a network that the router can reach.

Citrix Server

To create a new list, click **Add** and provide the required information in the dialog
displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this
table.

Summary

This window displays a summary of the Cisco IOS SSL VPN configuration that you have created. Click **Finish** to deliver the configuration to the router, or click **Back** to return to a wizard window to make changes.

To see the CLI commands that you are delivering to the router, go to **Edit > Preferences**, and check **Preview commands before delivering to router.**

Editing SSL VPN Connections

To edit an SSL VPN connection, complete the following tasks:

Step 1   If you want to review the Cisco IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **VPN**.

Step 4   In the VPN tree, click SSL VPN.

Step 5   Click **Edit SSL VPN**.

Step 6   Choose the SSL VPN connection that you want to edit.

Step 7   Click **Edit**. Then, make changes to the settings in the displayed dialogs.

Step 8   Click **OK** to close the dialog and send the changes to the router.

Step 9   If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it.

Editing SSL VPN Connection Reference describes the configuration screens.

Editing SSL VPN Connection Reference

The topics in this section describe the SSL VPN Edit screens.

- Edit SSL VPN
- SSL VPN Context
- Designate Inside and Outside Interfaces
- Select a Gateway
- Context: Group Policies
- Group Policy: General Tab
- Group Policy: Clientless Tab
- Group Policy: Thin Client Tab
- Group Policy: SSL VPN Client (Full Tunnel) Tab
- Advanced Tunnel Options
- DNS and WINS Servers
- Context: HTML Settings
- Select Color
- Context: NetBIOS Name Server Lists
- Add or Edit a NBNS Server List
- Add or Edit an NBNS Server
- Context: Port Forward Lists
- Add or Edit a Port Forward List
- Context: URL Lists
- Add or Edit a URL List
- Context: Cisco Secure Desktop
- SSL VPN Gateways
- Add or Edit a SSL VPN Gateway
- Packages
- Install Package

Edit SSL VPN

The Edit SSL VPN window allows you modify or create Cisco IOS SSL VPN configurations. The top portion of the tab lists the configured Cisco IOS SSL VPN contexts. The bottom portion displays details for that context.

Click Cisco IOS SSL VPN to get an overview of the Cisco IOS SSL VPN features that Cisco SDM supports.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

Click Cisco IOS SSL VPN Contexts, Gateways, and Policies for a description of how the components of a Cisco IOS SSL VPN configuration work together.

SSL VPN Contexts

This area displays the Cisco IOS SSL VPN contexts configured on the router. Click a context in this area to display the detailed information for it in the lower part of the window. Add a new context by clicking **Add** and entering information in the dialog displayed. Edit a context by selecting it and clicking **Edit**. Remove a context and its associated group policies by selecting it and clicking **Delete**.

You can enable a context that is not in service by choosing it and clicking **Enable**. Take a context out of service by choosing it and clicking **Disable**.

The following information is displayed for each context.

Name

The name of the Cisco IOS SSL VPN context. If you created the context in the Cisco IOS SSL VPN wizard, the name is the string that you entered in the IP Address and Name window.

Gateway

The gateway that the context uses contains the IP address, and digital certificate that the Cisco IOS SSL VPN context will use.

Domain

If a domain has been configured for the context, it is displayed in this column. If a domain is configured, users must enter that domain in the web browser to access the portal.

Status

Contains icons for quick status identification.

Administrative Status

Textual description of status.

- In Service—Context is in service. Users specified in policies configured under the context can access their Cisco IOS SSL VPN portal.

- Not in Service—Context is not in service. Users specified in policies configured under the context cannot access their Cisco IOS SSL VPN portal.

Sample Display

The following table shows a sample Cisco IOS SSL VPN contexts display.

Name	Gateway	Domain	Status	Administrative Status
WorldTravel	Gateway1	wtravel.net		In Service
A+Insurance	Gateway2	aplus.com		Not in Service

Details about SSL VPN Context: *Name*

This area displays details about the context with the name *name* that you selected in the upper part of the window. You can modify the settings that you see by clicking **Edit** in the top part of the window.

SSL VPN Context

Use this window to add or edit a Cisco IOS SSL VPN context.

Field Reference

Table 21-1 describes the fields in this screen.

Table 21-1   SSL VPN Context Fields

Element	Description
Name	Enter the name of a new context, or choose the name of an existing context to edit it.
Associated Gateway	Select an existing gateway, or click **Create gateway** to configure a new gateway for the context. The gateway contains the IP address and digital certificate is used for this context. Each gateway requires a unique public IP address.
Domain	If you have a domain for this context, enter it in this field. Cisco IOS SSL VPN users will be able to use this domain name when accessing the portal, instead of an IP address. An example is mycompany.com.
Authentication List	Choose the AAA method list to be used to authenticate users to this context.
Authentication Domain	Enter the domain name that is to be appended to the username before it is sent for authentication. This domain must match the domain used on the AAA server for the users that will be authenticated for this context.
Enable Context	Check **Enable Context** if you want the context to be enabled when you finish configuring it. You do not have to return to this window to disable it if you enable it here. You can enable and disable individual contexts in the Edit SSL VPN tab.
Maximum Number of Users	Enter the maximum number of users that should be allowed to use this context at one time.
VRF Name	Enter the VPN Routing and Forwarding (VRF) name for this context. This VRF name must have already been configured on the router.

Table 21-1   SSL VPN Context Fields (continued)

Element	Description
Default Group Policy	Select the policy that you want to use as the default group policy. The default group policy will be used for users who have not been included in any policy configured on the AAA server.
Enable RADIUS Accounting	Check **Enable RADIUS Accounting** to enable this feature for the context that you are editing. If this option is disabled, the AAA authentication list chosen for the context does not include any configured AAA servers. You must choose a different authentication list, or configure a new one.
	To add the information for an AAA to the router configuration, click **Additional Tasks > AAA > AAA Servers > Add**. Enter the IP address and other required information in the displayed dialog. The AAA server information you enter becomes available for use in authentication lists.

Designate Inside and Outside Interfaces

An ACL that is applied to an interface on which a Cisco IOS SSL VPN connection is configured may block the SSL traffic. Cisco SDM can automatically modify the ACL to allow this traffic to pass through the firewall. However, you must indicate which interface is the inside (trusted) interface, and which is the outside (untrusted) interface for Cisco SDM to create the Access Control Entry (ACE) that will allow the appropriate traffic to pass through the firewall.

Check **Inside** if the listed interface is a trusted interface, and check **Outside** if it is an untrusted interface.

Select a Gateway

Select an existing gateway from this window. This window provides you with the information you need to determine which gateway to select. It displays the names and IP addresses of all gateways, the number of contexts each is associated with, and whether the gateway is enabled or not.

Context: Group Policies

This window displays the group policies configured for the chosen Cisco IOS SSL VPN context. Use the **Add**, **Edit**, and **Delete** buttons to manage these group policies.

For each policy, this window shows the name of the policy and whether the policy is the default group policy. The default group policy is the policy assigned to a user who has not been included in another policy. You can change the group policy by returning to the Context window and selecting a different policy as the default.

Click a policy in the list to view details about the policy in the lower part of the window. For a description of these details, click the following links

Group Policy: General Tab

Group Policy: Clientless Tab

Group Policy: Thin Client Tab

Group Policy: SSL VPN Client (Full Tunnel) Tab

Click here to learn more

Click the link in the window for important information. To get to that information from this help page, click Learn More About Group Policies.

Group Policy: General Tab

When creating a new group policy, you must enter information in each field of the General tab.

Field Reference

Table 21-2 describes the fields in this screen.

Table 21-2   General Tab Fields

Element	Description
Name	Enter a name for the group policy, for example Engineering, Human Resources, or Marketing.
Make this the default group policy for context	Check if you want to make this the default group policy. The default group policy is the policy assigned to a user who is not included in another policy. If you check this checkbox, this policy will be shown as the default policy in the Group Policy window.
Timeouts	
Idle Timeout	Enter the number of seconds that the client can remain idle before the session is terminated.
Session Timeout	Enter the maximum number of seconds for a session, regardless of the activity on the session.
Application ACL	
Application ACL	SSLVPN uses application ACLs to specify permitted and denied URLs for groups. Choose a configured application ACL for this group. To configure application ACLs, go to the SSL VPN Context tree, click **App ACL** to display the Access Control List window, and then click **Add**.
View	Click **View** to display the details for the chosen application ACL.

Group Policy: Clientless Tab

Clientless Citrix allows users to run applications on remote servers in the same way that they would run them locally, without client software needing to be installed on the remote systems using these applications. The Citrix software must be installed on one or more servers on a network that the router can reach.

Enter information if you want Cisco IOS SSL VPN clients to be able to use Clientless Citrix.

Field Reference

Table 21-3 describes the fields in this screen.

Table 21-3 *Clientless Tab Fields*

Element	Description
Clientless Web Browsing	
Action URL List	Select one or more URL lists that you want to display in the portal that the users in this group will see. URLs in the list that you specify will be displayed in the portal.
View	To examine a URL list, choose a name from the list and click **View**.
Add	To add a URL list or a Citrix Server list, click **Add** and choose the option that you want
Hide URL bar in the portal page	If you want to restrict users to URLs in the list, and prevent them from entering additional URLs, click **Hide URL bar in the portal page**.
Enable URL Obfuscation	Click **Enable URL Obfuscation** to enable this feature for the group policy. When URL obfuscation is enabled, end users do not see the the path to the web server or other internal resource in the web page that they are using. Instead, they see an obfuscated path that provides no information about the network.
Enable Citrix	Click **Enable Citrix** to enable Clientless Citrix for the group policy. Citrix allows users to run applications such as Microsoft Word or Excel on remote servers in the same way that they would run them locally, without the need for client software on the PC. The Citrix software must be installed on one or more servers on a network that the router can reach.
Enable CIFS	
Choose **Enable CIFS** if you want to allow group members to browse files on MS Windows servers in the corporate network. When you enable CIFS, the options that follow are enabled.	
Read	Click **Read** to allow group members to read files.
Write	Click **Write** to allow group members to make changes to files.

Table 21-3   *Clientless Tab Fields*

Element	Description
NBNS Server List	You must specify the NBNS server list that will enable the appropriate files to be displayed to these users. Choose the NBNS Server list to use for this group. To configure a list, click **NETBIOS Name Server Lists** in the SSL VPN Context tree and click **Add** to configure a list.
View	To verify the contents of a WINS server list, choose the list and click **View**.

Group Policy: Thin Client Tab

Make settings in this tab if you want to configure Thin Client, also known as port forwarding, for members of this group.

Field Reference

Table 21-4 describes the fields in this screen.

Table 21-4   *Thin Client Tab Fields*

Element	Description
Enable Thin Client	Click **Enable Thin Client** (**Port Forwarding**) and specify a port forward list to enable this feature. At least one port forward list must be configured for the Cisco IOS SSL VPN context under which this group policy is configured.
View	To examine the port forwarding list you have chosen, click **View**.
Automatically Download Applet	The Automatically Download Applet option causes the Thin Client applet to be downloaded automatically to clients when they have logged on. This option is checked by default.

Group Policy: SSL VPN Client (Full Tunnel) Tab

Make setting in this tab if you want to enable the group members to download and use full-tunnel client software.

Note You must specify the location of the Full Tunnel client software by clicking **Packages** in the SSL VPN tree, specifying the location of the install bundle, and then clicking **Install**.

Enable Full Tunnel connections by choosing **Enable** from the list. If you want to require Full Tunnel connections, choose **Required**. If you choose **Required**, Clientless and Thin Client communication will work only if the Cisco IOS SSL VPN client software is successfully installed on the client PC.

IP address pool from which clients will be assigned an IP address

Clients who establish Full Tunnel communication are assigned IP addresses by the router. Specify the name of the pool, or click the **...** button to create a new pool from which the router can assign addresses.

Keep full-tunnel client software installed on client's PC Checkbox

Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this checkbox, clients download the software each time they establish communication with the gateway.

Renegotiate Key field

Enter the number of seconds after which the tunnel should be brought down so that a new SSL key can be negotiated and the tunnel can be reestablished.

ACL to restrict access for users in this group to corporate resources

You can choose or create an access list (ACL) that specifies the resources on the corporate network that group members will be restricted to.

Home page client should see when a web browser is opened with full tunnel software installed

Enter the URL to the home page that is to be displayed to full-tunnel clients in this group.

Dead Peer Detection Timeouts

Dead Peer Detection (DPD) allows a system to detect a peer that is no longer responding. You can set separate timeouts that the router can use to detect clients that are no longer responding, and servers that are no longer responding. The range for both is from 0 to 3600 seconds.

Configure DNS and WINS servers Button

Click to display the DNS and WINS Servers dialog, which allows you to provide the IP addresses of the DNS and WINS servers on the corporate intranet that clients should use when accessing intranet hosts and services.

Configure Advanced Tunnel Options Button

Click to display the Advanced Tunnel Options dialog, which allows you to configure tunnel settings for split tunneling, split DNS, and proxy server settings for clients using Microsoft Internet Explorer.

Advanced Tunnel Options

The settings that you make in this dialog allow you to control the traffic that is encrypted, specify the DNS servers on the corporate intranet, and specify the proxy server settings that are to be sent to client browsers.

Split Tunneling

Encrypting all tunnel traffic may take excessive system resources. Split tunneling allows you to specify the networks whose traffic should be encrypted, and exempt traffic destined for other networks from encryption. You can either specify which tunnel traffic is to be encrypted or you can specify the traffic that is *not* to be encrypted and allow the router to encrypt all other tunnel traffic. You can only build one list; included and excluded traffic are mutually exclusive.

Click **Include traffic** and use the **Add**, **Edit**, and **Delete** keys to build a list of destination networks whose traffic is to be encrypted. Or, click **Exclude traffic** and build a list of the destination networks whose traffic is *not* to be encrypted.

Click **Exclude Local LANs** to explicitly exclude from encryption client traffic destined for LANs that the router is connected to. If there are networked printers on these LANs, you must use this option.

The section "Learn More About Split Tunneling" contains more information about this topic.

Split DNS

If you want Cisco IOS SSL VPN clients to use the DNS server in the corporate network only to resolve specific domains, you can enter those domains in this area. They should be domains within the corporate intranet. Separate each entry with a semicolon and do not use carriage returns. Here is a sample list of entries:

yourcompany.com;dev-lab.net;extranet.net

Clients must use the DNS servers provided by their ISPs to resolve all other domains.

Browser Proxy Settings

The settings in this area are sent to client Microsoft Internet Explorer browsers with full tunnel connections. These settings have no effect if clients use a different browser.

Do not use proxy server

Click to instruct Cisco IOS SSL VPN client browsers not to use a proxy server.

Auto-detect proxy settings

Click if you want the Cisco IOS SSL VPN client browsers to auto detect proxy server settings.

Bypass proxy settings for local addresses

Click if you want clients connecting to local addresses to be able to bypass normal proxy settings.

Proxy Server

Enter the IP address of the proxy server and the port number for the service that it provides in these fields. For example, if the proxy server supports FTP requests, enter the IP address of the proxy server and port number 21.

Do not use proxy server for addresses beginning with

> If you do not want clients to use proxy servers when sending traffic to specific IP addresses or networks, you can enter them here. Use a semicolon to separate each entry. For example, if you do not want clients to use a proxy server when connecting to any server in the 10.10.0.0 or 10.11.0.0 networks, enter 10.10;10.11. You can enter as many networks as you want.

DNS and WINS Servers

> Enter the IP addresses for the corporate DNS and WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet.

> Provide addresses for primary and for secondary DNS servers and WINS servers.

DNS and WINS Servers

> Enter the IP addresses for the corporate DNS and WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet.

> Provide addresses for primary and for secondary DNS servers and WINS servers.

Context: HTML Settings

> The settings that you make in this window control the appearance of the portal for the selected Cisco IOS SSL VPN context.

Select theme

> You can specify the appearance of the portal by selecting a predefined theme instead of by selecting each color yourself. When you select a theme, the settings for that theme are displayed in the fields associated with the **Customize** button.

Customize Button

> Click if you want to select each color used in the portal and specify a login message and title. If you selected a predefined theme, the values for that theme are displayed in the fields in this section. You can change these values, and the

values you enter are used in the portal for the selected context. Changes that you make in this window only affect the portal you are creating. They do not change the default values for the theme.

Login Message

Enter the login message that you want clients to see when their browsers display the portal. For example:

```
Welcome to the company-name network. Log off if you are not an
authorized user.
```

Title

Enter the title that you want to give the portal. For example:

```
Company-name network login page
```

Background Color for Title

The default value for the background color that appears behind the title is #9999CC. Change this value by clicking the **...** button and selecting a different color.

Background Color for Secondary Titles

The default value for the background color that appears behind the title is #9729CC. Change this value by clicking the **...** button and selecting a different color, or by entering the hexadecimal value for a different color.

Text Color

The default value for the text color is white. Change this value by clicking the down arrow and selecting a different color.

Secondary Text Color

The default value for the secondary text color is black. Change this value by clicking the down arrow and selecting a different color.

Logo File

If you have a logo that you want to display on the portal, click the **...** button to browse for it on your PC. It is saved to router flash after you click **OK**, and will appear in the upper-left corner of the portal.

Preview Button

Click to see a preview of the portal as it will look with the predefined theme or custom values you have specified.

Select Color

Click **Basic** to select a predefined color, or click **RGB** to create a custom color.

Basic

Select the color that you want to use from the palette on the left. The color you select appears in the large square in the right side of the dialog.

RGB

Use the Red, Green, and Blue sliders in combination to create a custom color. The color you create appears in the large square in the right side of the dialog.

Context: NetBIOS Name Server Lists

View all the NetBIOS name server lists that are configured for the selected Cisco IOS SSL VPN context in this window. CIFS uses NetBIOS servers to display the corporate Microsoft Windows file system to Cisco IOS SSL VPN users.

Each name server list configured for the context is shown in the **NetBIOS Name Server Lists** area. Use the **Add**, **Edit**, and **Delete** buttons to manage these lists. Click a list name to view the contents of the list in the **Details of NetBIOS Name Server** area.

Add or Edit a NBNS Server List

Create or maintain a NBNS server list in this window. You must enter a name for each list that you create, and provide the IP address, timeout and number of retries to attempt for each server in the list. One server in each list must be designated as the master server.

Each server in the list is displayed in this dialog, along with its master status, timeout, and retries values.

Add or Edit an NBNS Server

You must enter the IP address of each server, along with the number of seconds that the router is to wait before attempting to connect to the server again, and the number of times the router is to attempt to contact the server.

Check **Make this server the master server** if you want this server to be the first server that the router contacts on the list.

Context: Port Forward Lists

Configure the port forwarding lists for the selected context in this window. The lists can be associated to any group policy configured under the selected context. Port forward lists reveal TCP application services to Cisco IOS SSL VPN clients.

The upper part of the window displays the port forward lists configured for the selected context. Click a list name to display the details for the list in the lower part of the window.

The window displays the IP address, port number used, corresponding port number on the client, and a description if one was entered.

Add or Edit a Port Forward List

Create and maintain port forward lists in this window. Each list must be given a name, and contain at least one server entry. Use the **Add**, **Edit**, and **Delete** buttons to create, modify, and remove entries from the list.

Context: URL Lists

URL lists specify which links can appear on the portal for users in a particular group. Configure one or more URL lists for each context, then use the group policy windows to associate these lists with specific group policies.

The upper part of the window displays all the URL lists configured for the context. The lower part of the window displays the contents of the selected list. For each list, it displays the heading that is displayed at the top of the URL list, and each URL that is in the list.

Use the **Add**, **Edit**, and **Delete** buttons to create and manage URL lists.

Add or Edit a URL List

You must enter a name for each URL list, and heading text that will appear at the top of the URL list.

Heading text should describe the overall contents of the links in the list. For example, if a URL list provides access to the health plan web pages and insurance web pages, you might use the heading text `Benefits`.

Use the **Add** button to create a new entry for the list, and the **Edit** and **Delete** buttons to maintain the list. Each entry that you add appears in the list area.

Context: Cisco Secure Desktop

Cisco Secure Desktop encrypts cookies, browser history files, temporary files, and e-mail attachments that could create security problems if left unencrypted. After a Cisco IOS SSL VPN session is terminated, Cisco Secure Desktop removes the data using a Department of Defense sanitation algorithm.

Click **Enable Cisco Secure Desktop** to allow all users of this context to download and use **Cisco Secure Desktop**. This window displays a message if the install bundle for this software is not found on the router.

To load the install bundle for Cisco Secure Desktop on the router, click Packages in the Cisco IOS SSL VPN tree and follow the instructions in the window.

SSL VPN Gateways

This window displays the Cisco IOS SSL VPN gateways configured on the router and enables you to modify existing gateways and configure new ones. A Cisco IOS SSL VPN gateway is the user portal to the secure network.

SSL VPN Gateways

This area of the window lists the Cisco IOS SSL VPN gateways that are configured on the router. It shows the name and IP address of the gateway, the number of contexts configured to use the gateway, and the status of the gateway.

    The gateway is enabled and in service.

    The gateway is disabled and out of service.

Click a gateway to view details about it in the lower part of the window. Enable a gateway that is **Disabled** by choosing it and clicking **Enable**. Take an enabled gateway out of service by choosing it and clicking **Disable**. To edit a gateway, select the gateway and click the **Edit** button. To remove a gateway, choose the gateway and click the **Delete** button.

Details of SSL VPN Gateway

This area of the window displays configuration details about the gateway selected in the upper part of the window, and the names of the Cisco IOS SSL VPN contexts that are configured to use this gateway.

For more information on gateway configuration details, click Add or Edit a SSL VPN Gateway. For more information on contexts, click SSL VPN Context.

Add or Edit a SSL VPN Gateway

Create or edit a Cisco IOS SSL VPN gateway in this window.

Gateway Name

The gateway name uniquely identifies this gateway on the router, and is the name used to refer to the gateway when configuring Cisco IOS SSL VPN contexts.

IP Address

Choose or enter the IP address that the gateway is to use. This must be a public IP address, and cannot be an address used by another gateway on the router.

Digital Certificate

Choose the certificate that is to be sent to Cisco IOS SSL VPN clients for SSL authentication.

HTTP Redirect Checkbox

Uncheck if you do not want HTTP redirect to be used. HTTP redirect automatically redirects HTTP requests to port 443, the port used for secure Cisco IOS SSL VPN communication.

Enable Gateway Checkbox

Uncheck if you do not want to enable the gateway. You can also enable and disable the gateway from the SSL VPN Gateways window.

Packages

This window enables you to obtain software install bundles that must be downloaded to Cisco IOS SSL VPN clients to support Cisco IOS SSL VPN features, and to load them on the router. You can also use this window to remove install bundles that have been installed.

Follow the steps described in the window to download the install bundles from Cisco.com to your PC, and then copy them from your PC to the router. If you need to obtain any of the install bundles, start with Step 1 by clicking on the link to the download site.

> **Note** Access to these download sites requires a CCO username and password. If you don't have a CCO username and password, you can obtain one by clicking Register at the top of any Cisco.com webpage, and completing the form that is displayed. Your username and password will be mailed to you.

If you have already loaded install bundles onto your PC or the router, complete steps 2 and 3 to specify the current location of the install bundles and copy them to router flash.

Click the **...** button in each section to specify the current location of the install bundle.

After you specify the current location, and where you want to copy it to in router flash, click **Install**.

After the bundles have been loaded onto the router, the window displays name, version, and build date information about the package. If an administration tool is available with the package, the window displays a button enabling you to run this tool.

The Cisco IOS SSL VPN client install bundle is available from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

The Cisco Secure Desktop install bundle is available from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Install Package

Specify the current location of an install bundle by browsing for it in this window. If the install bundle is already located on the router, click **Router** and browse for it. If it is located on the PC, click **My Computer** and browse for it. When you have specified the current location of the install bundle, click **OK**.

The location will be visible in the Packages window.

Additional Help Topics

The help topics in this section provide additional background information, and procedures that you may need to perform manually.

This section contains the following topics:

- Cisco IOS SSL VPN Contexts, Gateways, and Policies
- Learn More about Port Forwarding Servers
- Learn More About Group Policies
- Learn More About Split Tunneling
- How do I verify that my Cisco IOS SSL VPN is working?
- How do I configure a Cisco IOS SSL VPN after I have configured a firewall?
- How do I associate a VRF instance with a Cisco IOS SSL VPN context?

Cisco IOS SSL VPN Contexts, Gateways, and Policies

Cisco SDM provides an easy way to configure Cisco IOS SSL VPN connections for remote users. However, the terminology used in this technology can be confusing. This help topic discusses the Cisco IOS SSL VPN terms used in Cisco SDM configuration windows and describes how Cisco IOS SSL VPN components work together. An example of using the Cisco IOS SSL VPN wizard and edit windows in Cisco SDM is also provided.

Before discussing each component individually, it is helpful to note the following:

- One Cisco IOS SSL VPN context can support multiple group policies.

- Each context must have one associated gateway.

- One gateway can support multiple contexts.

- If there is more than one group policy on the router, a AAA server must be used for authentication.

Cisco IOS SSL VPN Contexts

A Cisco IOS SSL VPN context identifies resources needed to support SSL VPN tunnels between remote clients and a corporate or private intranet, and supports one or more group policies. A Cisco IOS SSL VPN context provides the following resources:

- An associated Cisco IOS SSL VPN gateway, which provides an IP address that clients can reach and a certificate used to establish a secure connection.

- Means for authentication. You can authenticate users locally, or by using AAA servers.

- The HTML display settings for the portal that provides links to network resources.

- Port forwarding lists that enable the use of Thin Client applets on remote clients. Each list should be configured for use in a specific group policy.

- URL lists that contain links to resources in the corporate intranet. Each list should be configured for use in a specific group policy.

- NetBIOS Name Server lists. Each list should be configured for use in a specific group policy.

These resources are available when configuring Cisco IOS SSL VPN group policies.

A Cisco IOS SSL VPN context can support multiple group policies. A Cisco IOS SSL VPN context can be associated with only one gateway.

Cisco IOS SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides a reachable IP address and certificate for one or more Cisco IOS SSL VPN contexts. Each gateway configured on a router must be configured with its own IP address; IP addresses cannot be shared among gateways. It is possible to use the IP address of a router interface, or

another reachable IP address if one is available. Either a digital certificate or a self-signed certificate must be configured for gateways to use. All gateways on the router can use the same certificate.

Although one gateway can serve multiple Cisco IOS SSL VPN contexts, resource constraints and IP address reachability must be taken into account.

Cisco IOS SSL VPN Policies

Cisco IOS SSL VPN group policies allow you to accommodate the needs of different groups of users. A group of engineers working remotely needs access to different network resources than sales personnel working in the field. Business partners and outside vendors must access the information they need to work with your organization, but you must ensure that they do not have access to confidential information or other resources they do not need. Creating a different policy for each of these groups allows you provide remote users with the resources they need, and prevent them from accessing other resources.

When you configure a group policy, resources such as URL lists, Port Forwarding lists, and NetBIOS name server lists configured for the policy's associated context are available for selection.

If there is more than one group policy configured on the router, you must configure the router to use a AAA server to authenticate users and to determine which policy group a particular user belongs to. Click Learn More About Group Policies for more information.

Example

In this example, a user clicks **Create a new SSL VPN** and uses the wizard to create the first Cisco IOS SSL VPN configuration on the router. Completing this wizard creates a new context, gateway, and group policy. The following table contains the information the user enters in each wizard window, and the configuration that Cisco SDM creates with that information.

Table 21-5   *Creating a New SSLVPN*

Cisco IOS SSL VPN Wizard Window	Configuration
Create SSL VPN Window	
Prerequisite Tasks area indicates that digital certificates are not configured on the router. User clicks **self signed certificate** and configures a certificate in the Persistent Self Signed Certificate dialog. The user does not change the Cisco SDM-supplied name Router_Certificate. User clicks **Create new SSL VPN**.	Cisco SDM configures a self-signed certificate named "Router_Certificate" that will be available for use in all Cisco IOS SSL VPN configurations.
IP Address and Name Window	
User enters the following information: IP Address: 172.16.5.5 Name: Asia Check **Enable secure SDM access through 192.168.1.1**. Certificate: **Router_Certificate**	Cisco SDM creates a context named "Asia." Cisco SDM creates a gateway named "gateway_1" that uses the IP address 172.16.5.5 and Router_Certificate. This gateway can be associated with other Cisco IOS SSL VPN contexts. Users will access the Cisco IOS SSL VPN portal by entering http://172.16.5.5/Asia. If this gateway is associated with additional contexts, the same IP address will be used in the URL for those contexts. For example if the context Europe is also configured to use gateway_1, users enter https://172.16.5.5/Europe to access the portal. After the configuration is delivered to the router, users must enter http://172.16.5.5:4443 to launch Cisco SDM using this IP address. Cisco SDM also begins to configure the first group policy, named policy_1.
User Authentication Window	

Table 21-5   Creating a New SSLVPN (continued)

Cisco IOS SSL VPN Wizard Window	Configuration
User chooses **Locally on this router**. User adds one user account to the existing list.	Cisco SDM creates the authentication list "sdm_vpn_xauth_ml_1." This list will be displayed in the Cisco IOS SSL VPN Contexts window when the user completes the wizard. Those users listed in the User Authentication window are the members of this authentication list, and will be governed by policy_1.
Configure Intranet Websites Window	
User configures the URL list Ulist_1. The heading is "Taiwan."	The URL list with the heading Taiwan will be visible in the portal that users in "sdm_vpn_xauth_ml_1" see when they log in. The URL list will be available for configuration in other group policies configured under the context "Asia."
Enable Full Tunnel Window	
User clicks **Enable Full Tunnel**, and selects a predefined address pool. No advanced options are configured.	Client PCs will download Full Tunnel client software when they log in for the first time, and a full tunnel is established between the PC and the router when the user logs in to the portal.
Customize SSL VPN Portal Window	
User chooses **Ocean Breeze**.	Cisco SDM configures the HTTP display settings with this color scheme. The portal displayed when policy_1 users log in uses these settings. These portal settings also apply to all policies configured under the context "Asia." The user can customize the HTTP display settings in the Edit SSL VPN windows after completing the wizard.
SSL VPN Passthrough Configuration Window	
User checks **Allow SSL VPN to work with NAC and Firewall**	Cisco SDM adds an ACL with the following entry. `permit tcp any host 172.16.5.5 eq 443`

Table 21-5   Creating a New SSLVPN (continued)

Cisco IOS SSL VPN Wizard Window	Configuration
Summary Window	

The Summary window displays the information shown at the right. Additional details can be viewed in the Edit SSL VPN windows.	SSL VPN Policy Name: policy_1
	SSL VPN Gateway Name: gateway_1
	
	User Authentication Method List: Local
	
	Full Tunnel Configuration
	    SVC Status: Yes
	    IP Address Pool: Pool_1
	    Split Tunneling: Disabled
	    Split DNS: Disabled
	    Install Full Tunnel Client: Enabled

When this configuration is delivered, the router has one Cisco IOS SSL VPN context named Asia, one gateway named gateway_1, and one group policy named policy_1. This is displayed in the Edit SSL VPN window as shown in the following table:

Name	Gateway	Domain	Status	Administrative Status
Asia	gateway_1	Asia		In Service

Details about SSL VPN context Asia:

Item Name	Item Value
Group Policies	
policy_1	
Services	URL Mangling, Full Tunnel
URLs exposed to Users	http://172.16.5.5/pricelist
	http://172.16.5.5/catalog
Servers Exposed to users	<None>
WINS servers	<None>

policy_1 provides the basic Cisco IOS SSL VPN service of URL mangling, and specifies that a full tunnel be established between clients and the router. No other features are configured. You can add features to policy_1, such as Thin Client and Common Internet File System by choosing **Configure advanced features for an existing SSL VPN**, choosing **Asia** and **policy_1** in the Select the Cisco IOS SSL VPN user group window, then choosing the features in the Advanced Features window. Additional URL lists can also be configured in this wizard.

You can create a new group policy under context "Asia" by choosing **Add a new policy to an existing SSL VPN for a new group of users**.

You can customize settings and the policies configured for context Asia by choosing Asia in the context list and clicking **Edit**. The Edit SSL VPN Context Asia window displays a tree that allows you to configure more resources for the context, and to edit and configure additional policies. You can edit the settings for gateway_1 by clicking **SSL VPN Gateways** under the SSL VPN node, selecting gateway_1, then clicking **Edit**.

Learn More about Port Forwarding Servers

Port forwarding enables a remote Cisco IOS SSL VPN user to connect to static ports on servers with private IP addresses on the corporate intranet. For example, you can configure port forwarding on a router to give remote users Telnet access to a server on the corporate intranet. To configure port forwarding, you need the following information:

- The IP address of the server.
- The static port number on the server.
- The remote port number for the client PC. In the dialog, Cisco SDM supplies a port number that is safe to use.

To allow users to use Telnet to connect to a server with the IP address 10.0.0.100 (port 23) for example, you would create a port mapping entry with the following information:

Server IP address: 10.0.0.100

Server port on which user is connecting: 23

Port on client PC: Cisco SDM-supplied value. 3001 for this example.

Description: SSL VPN Telnet access to server-a. This description will be on the portal.

When the client's browser connects to the gateway router, a portal applet is downloaded to the client PC. This applet contains the server's IP address and static port number, and the port number that the client PC is to use. The applet does the following:

- Creates a mapping on the client PC that maps traffic for port 23 on 10.0.0.100 to the PC's loopback IP address 127.0.0.1, port 3001.

- Listens on port 3001, IP address 127.0.0.1

When the user runs an application that connects to port 23 on 10.0.0.100, the request is sent to 127.0.0.1 port 3001. The portal applet listening on that port and IP address gets this request and sends it over the Cisco IOS SSL VPN tunnel to the gateway. The gateway router forwards it to the server at 10.0.0.100, and sends return traffic back to the PC.

Learn More About Group Policies

Cisco IOS SSL VPN group policies define the portal and links for the users included in those policies. When a remote user enters the Cisco IOS SSL VPN URL they have been given, the router must determine which policy the user is a member of so that it can display the portal configured for that policy. If only one Cisco IOS SSL VPN policy is configured on the router, it can authenticate users locally or using a AAA server, and then display the portal.

However, if more than one policy is configured, the router must rely on a AAA server to determine which policy to use each time a remote user attempts to log in. If you have configured more than one Cisco IOS SSL VPN group policy, you must configure at least one AAA server for the router, and you must configure a policy on that server for each group of users for which you created a Cisco IOS SSL VPN policy. The policy names on the AAA server must be the same as the names of the group policies configured on the router, and they must be configured with the credentials of the users who are members of the group.

For example, if a router has been configured with local authentication for Bob Smith, and only the group policy Sales has been configured, there is only one portal available to display when Bob Smith attempts to log in. However, if there are three Cisco IOS SSL VPN group policies configured, Sales, Field, and Manufacturing, the router cannot, by itself, determine which policy group Bob Smith is a member of. If a AAA server is configured with the proper information

for those policies, the router can contact that server, and receive the information that Bob Smith is a member of the group Sales. The router can then display the correct portal for the Sales group.

For information on how to configure the AAA server, see the "Configuring RADIUS Attribute Support for SSL VPN" section in the *SSL VPN Enhancements* document at the following link:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00 805eeaea.html#wp1396461

Learn More About Split Tunneling

When a Cisco IOS SSL VPN connection is set up with a remote client, all traffic that the client sends and receives may travel through the Cisco IOS SSL VPN tunnel, including traffic that is not on the corporate intranet. This can degrade network performance. Split tunneling allows you to specify the traffic that you want to send through the Cisco IOS SSL VPN tunnel and allow other traffic to remain unprotected and be handled by other routers.

In the Split Tunneling area, you can specify the traffic to *include* in the Cisco IOS SSL VPN and exclude all other traffic by default, or you can specify the traffic to *exclude* from the CCisco IOS SSL VPN and include all other traffic by default.

For example, suppose that your organization uses the 10.11.55.0 and the 10.12.55.0 network addresses. Add these network addresses to the Destination Network list, then click the **Include traffic** radio button. All other Internet traffic, such as traffic to Google or Yahoo, would go direct to the Internet.

Or suppose it is more practical to exclude traffic to certain networks from the Cisco IOS SSL VPN tunnel. In that case, enter the addresses for those networks in the Destination Networks list, then click the **Exclude traffic** radio button. All traffic destined for the networks in the Destination Networks list is sent over nonsecure routes, and all other traffic is sent over the Cisco IOS SSL VPN tunnel.

If users have printers on local LANs that they want to use while connected to the Cisco IOS SSL VPN, you must click **Exclude local LAN** in the Split Tunneling area.

✎

Note   The Destination Network list in the Split Tunneling area may already contain
network addresses. The traffic settings you make in the Split Tunneling area
override any settings previously made for the listed networks.

How do I verify that my Cisco IOS SSL VPN is working?

The best way to determine that a Cisco IOS SSL VPN context will provide the
access that you configured for users is to configure yourself as a user, then attempt
to access all the websites and services that the context is configured to provide for
them. Use the following procedure as a guide in setting up this test.

Step 1   Ensure that credentials you can use are included in all appropriate policies on the
AAA server.

Step 2   If you can do so, open a Cisco SDM session to the router so that you can monitor
the Cisco IOS SSL VPN traffic that you will create. This must be done on a
separate PC if the PC you use to test the Cisco IOS SSL VPN context is not in a
network from which you can access Cisco SDM. Go to **Monitor** > **VPN Status** >
SSL VPN.

Step 3   Enter the URL to each of the web portals that are configured for this Cisco IOS
SSL VPN context. Determine that each page has the appearance that you
configured for it, and that all links specified in the URL lists for the policy appear
on the page.

Step 4   Test all links and services that should be available to users included in this policy.
If any of the policies that you are testing provide for downloading Cisco Secure
Desktop or the Full Tunnel client software, enter the URLs to the web portals for
those policies and click the links that will require the download of this software.
Determine that the software downloads properly and that you are able to access
the services that a user should be able to access from these links.

Step 5   If you were able to establish a Cisco SDM session before you began testing, click
the branch for the context that you are testing and observe the Cisco IOS
SSL VPN traffic statistics in the Cisco IOS SSL VPN window.

Step 6   Based on the results of your tests, go back to Cisco SDM if necessary and fix any
configuration problems you discovered.

How do I configure a Cisco IOS SSL VPN after I have configured a firewall?

If you have already configured a firewall, you can still use the Cisco IOS SSL VPN wizards in Cisco SDM to create Cisco IOS SSL VPN contexts and policies. Cisco SDM validates the Cisco IOS SSL VPN CLI commands that it generates against the existing configuration on the router. If it detects an existing firewall configuration that would have to be modified to allow Cisco IOS SSL VPN traffic to pass through, you are informed. You can allow Cisco SDM to make the necessary modifications to the firewall, or you can leave the firewall intact and make the changes manually by going to **Configure** > **Firewall and ACL** > **Edit Firewall Policy/ACL** and entering the permit statements that allow Cisco IOS SSL VPN traffic to pass through the firewall.

How do I associate a VRF instance with a Cisco IOS SSL VPN context?

VPN Routing and Forwarding (VFR) instances maintain a routing table and a forwarding table for a VPN. You can associate a VRF instance or name with a Cisco IOS SSL VPN context by going to **Configure > VPN > SSL VPN > Edit SSL VPN**. Select the context that you want to associate a VRF instance to and click **Edit**. Select the name of the VRF instance in the dialog displayed.

> **Note**   The VRF instance must already be configured on the router.

SSL VPN Enhancements

This chapter explains how to configure SSL VPN enhancements available with

SSL VPN Reference

- SSL VPN Context: Access Control Lists
- Add or Edit Application ACL
- Add ACL Entry
- Action URL Time Range
- Add or Edit Action URL Time Range Dialog
- Add or Edit Absolute Time Range Entry
- Add or Edit Periodic Time Range Entry

SSL VPN Context: Access Control Lists

You can create Application ACLs to control access to specific URLs. This window displays the Application ACLs created for the selected context, and enables you to edit existing ACLs and create new ones.

Field Reference

Table 22-1 describes the fields in this screen.

Table 22-1   SSL VPN Access Control List Fields

Element	Description
Access Control List	
Add	To create an Application ACL, click **Add** and create the Application ACL in the displayed dialog.
Edit	To edit an Application ACL, choose the ACL and click **Edit**. Edit the ACL in the displayed dialog.
Delete	To delete an ACL choose the ACL and click **Delete**.
ACL Name	This table lists the names of the ACLs created for this context.
Details of ACL	
Action	One of the following: • Permit—Access to the URL in this entry is allowed. • Deny—Access to the URL in this entry is denied.
URL	The URL to which the ACL controls access.
Action URL Time Range	The range or periods of time that this ACL is in effect.

Add or Edit Application ACL

Create or edit an application ACL in this window. Cisco IOS SSL VPN uses application ACLs to specify permitted and denied URLs. One ACL can consist of multiple entries.

Field Reference

Table 22-2 describes the fields in this screen.

Table 22-2   Add or Edit SSL VPN Context ACL Fields

Element	Description
ACL Name	Enter a name for this ACL.
Add	To create an entry for this ACL, click **Add** and create the entry in the displayed dialog.
Edit	To modify an entry, select the entry and click **Edit**. Then modify it in the displayed dialog.
Delete	To remove an entry from this ACL, select the entry and click **Delete**.
List Area	
Action	One of the following: • Permit—Access to the URL in this entry is permitted. • Deny—Access to the URL in this entry is denied.
URL	The URL to which this ACL entry controls access.
Action URL Time Range	The name of the time range applied to this ACL entry.

Add ACL Entry

Add or Edit an ACL entry in this window.

Field Reference

Table 22-3 describes the fields in this screen.

Table 22-3   Add or Edit SSL VPN Context ACL Entry Fields

Element	Description
Action	Choose one of the following: • Permit—Allow access to the URL in this entry. • Deny—Deny access to the URL in this entry is denied.
URL	
Any	To have this ACL entry apply to any URL, click **Any**.

Table 22-3   Add or Edit SSL VPN Context ACL Entry Fields (continued)

Element	Description

Specific URL	To have this ACL entry apply to a URL that you specify, click **Specific URL**. Then, enter the URL in the field. Be sure to enter the entire URL. The following are examples of valid URLs:
	
	`http://www.cisco.com`
	`https://www.foo.com`
	`ftp://ftp.bad-down-loads.com`

Action URL Time Range	The action URL time range can specify the start and end date for the action specified, as well as the time periods that the action is to be in effect.To place a time range entry in this field, click the button to the right of the field and choose one of the following: • Add Time Range List—Choose this option to create a new time range entry. • Select Time Range List—Choose this option to select an existing time range entry. • Remove Time Range List—Choose this option to remove the current time range entry.

Action URL Time Range

Add time range lists in this window. Time range lists specify when permit or deny actions are to be applied.

Field Reference

Table 22-4 describes the fields in this screen.

Table 22-4   Action URL Time Range Fields

Element	Description
Time Range Entry	
Add	To create a time range entry, click **Add**, and create the entry in the displayed dialog.
Edit	To edit an entry, select the entry, and click Edit. Make changes to the entry in the displayed dialog.

Table 22-4   ***Action URL Time Range Fields (continued)***

Element	Description
Delete	To remove an entry, select the entry and click **Delete**.
Item Name	The Item Name list displays the time range entries configured for this context.
Details of Action URL Time Range	
The Details area displays additional information about the selected time range entry.	
Type	One of the following: • Absolute—The time range specifies an absolute date. There can be a start date, and there can be an end date, or both. • Periodic—The time range specifies days of the week, so that you can include some days and not others. It can also specify a start time and an end time.

Period	If the entry type is Periodic, this column shows which days are included. The following examples show possible entries:
	
	`daily`
	`weekdays`
	`Sun, Tue, Sat`

Start Time	The starting time and date is displayed for absolute entries, for example, 10:00 11 Nov 2007. The starting time is displayed for periodic entries, for example 8:00.
End Time	The end time and date is displayed for absolute entries, for example, 10:00 11 Dec 2007. The end time is displayed for periodic entries, for example 23:00.

Add or Edit Action URL Time Range Dialog

Create or edit a time range entry in this dialog. A time range entry can consist of multiple subentries.

Field Reference

Table 22-5 describes the fields in this screen.

Table 22-5   Time Range Fields

Element	Description
Time Range Name	Enter a name for the time range.
Time Range Entry List Area	
Type	One of the following: • Absolute—The time range specifies an absolute date. There can be a start date, and there can be an end date, or both. • Periodic—The time range specifies days of the week, so that you can include some days and not others. It can also specify a start time and an end time.

Period	If the entry type is Periodic, this column shows which days are included. The following examples show possible entries:
	
	`daily`
	`weekdays`
	`Sun, Tue, Sat`

Start	The starting time and date is displayed for absolute entries, for example, 10:00 11 Nov 2007. The starting time is displayed for periodic entries, for example 8:00.
End	The end time and date is displayed for absolute entries, for example, 10:00 11 Dec 2007. The end time is displayed for periodic entries, for example 23:00.
Add	To add an entry, click **Add,** and choose **Absolute**, or **Periodic**. If an absolute entry has been added, the Absolute option is disabled.
Edit	To edit a time range entry, select the entry and click **Edit**.
Delete	To remove a time range entry, select the entry and click **Delete**.

Add or Edit Absolute Time Range Entry

Create or edit an absolute time range entry in this window. The time range can have a start date, and end date, or both.

Field Reference

Table 22-6 describes the fields in this screen.

Table 22-6   Absolute Time Range Fields

Element	Description
Start	
To specify a start date, click **Start**, and enter a date and time.	
From Date	Enter the starting date in dd/mm/yyyy format. For example, entering 1/10/2007 specifies a start date of October 1, 2007.
Time	Enter the starting time in 24-hour format. For example, entering 13:00 specifies a starting time of 1:00 p.m.
End	
To specify an end date, click **End**, and enter a date and time	
Till Date	Enter the end date in dd/mm/yyyy format. For example, entering 1/1/2008 specifies an end date of January 1, 2008.
Time	Enter the ending time in 24-hour format. For example, entering 23:59 specifies an ending time of 11:59 p.m.

Add or Edit Periodic Time Range Entry

Create or edit a periodic time range entry in this window. You can specify which days to include in the range, and starting and ending days and times.

Field Reference

Table 22-7 describes the fields in this screen.

Table 22-7   Periodic Time Range Fields

Element	Description
Period	Choose one of the following: • Specific weekdays—To select specific days, choose this option, and then check the boxes next to the days of the week that you want to include. • weekdays—To include only Monday, Tuesday, Wednesday, Thursday, and Friday, choose this option. • weekend—To include only Saturday, and Sunday, choose this option. • daily—To include each day of the week, choose this option.
From Day	This option is available when you choose **Specific weekdays**. Check the box next to one day of the week to specify the From day.
Till Day	This option is available when you choose **Specific weekdays**, and you have specified one From day. Click the button and choose the Till day from the list. If more than one From day is checked, this option is disabled.
Duration	
Start Time	Enter the starting time in 24-hour format. For example, entering 13:00 specifies a starting time of 1:00 p.m.
End Time	Enter the ending time in 24-hour format. For example, entering 23:59 specifies an ending time of 11:59 p.m.

VPN Troubleshooting

Cisco SDM can troubleshoot VPN connections that you have configured. Cisco SDM reports the success or failure of the connection tests, and when tests have failed, recommends actions that you can take to correct connection problems.

The following link provides information on VPN troubleshooting using the CLI.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/useguide/u13_rtrb.htm

VPN Troubleshooting

This window appear when you are troubleshooting a site-to-site VPN, a GRE over IPSec tunnel, an Easy VPN remote connection, or an Easy VPN server connection.

> **Note** VPN Troubleshooting will not troubleshoot more than two peers for site-to-site VPN, GRE over IPsec, or Easy VPN client connections.

Tunnel Details

This box provides the VPN tunnel details.

Interface

Interface to which the VPN tunnel is configured.

Peer

The IP address or host name of the devices at the other end of the VPN connection.

Summary

Click this button if you want to view the summarized troubleshooting information.

Details

Click this button if you want to view the detailed troubleshooting information.

Activity

This column displays the troubleshooting activities.

Status

Displays the status of each troubleshooting activity by the following icons and text alerts:

The connection is up.

The connection is down.

Test is successful.

Test failed.

Failure Reason(s)

This box provides the possible reason(s) for the VPN tunnel failure.

Recommended action(s)

This box provides a possible action/solution to rectify the problem.

Close Button

Click this button to close the window.

Test Specific Client Button

> This button is enabled if you are testing connections for an Easy VPN server configured on the router. Click this button and specify the client to which you want to test connectivity.
>
> This button is disabled in the following circumstances:
>
> • The Basic testing is not done or has not completed successfully.
>
> • The IOS image does not support the required debugging commands.
>
> • The view used to launch Cisco SDM does not have root privileges.

What Do You Want to Do?

If you want to:	Do this:
Troubleshoot the VPN connection.	Click **Start** button. When test is running, **Start** button label will change to **Stop**. You have option to abort the troubleshooting while test is in progress.
Save the test report.	Click **Save Report** button to save the test report in HTML format. This button is disabled when the test is in progress.

VPN Troubleshooting: Specify Easy VPN Client

> This window allows you to specify the Easy VPN client which you want to debug.

IP Address

> Enter IP address of Easy VPN client you want to debug.

Listen for request for X minutes

> Enter the time duration for which Easy VPN Server has to listen to requests from Easy VPN client.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

VPN Troubleshooting: Generate Traffic

This window allows you to generate site-to-site VPN or Easy VPN traffic for debugging. You can allow Cisco SDM to generate VPN traffic or you can generate VPN traffic yourself.

VPN traffic on this connection is defined as

This area lists current VPN traffic on the interface.

Action
This column denotes whether the type of traffic is allowed in the interface.

Source
Source IP address.

Destination
Destination IP address.

Service
This column lists the type of traffic on the interface.

Log
This column indicates whether logging is enabled for this traffic.

Attributes
Any additional attributes defined.

Have SDM generate VPN Traffic

Select this option if you want Cisco SDM to generate VPN traffic on the interface for debugging.

> **Note** Cisco SDM will not generate VPN traffic when the VPN tunnel traffic is from non-IP based Access Control List (ACL) or when the applied and current CLI View is not root view.

Enter the IP address of a host in the source network

Enter the host IP address in the source network.

Enter the IP address of a host in the destination network

Enter the host IP address in the destination network.

I will generate VPN traffic from the source network

Select this option if you want to generate VPN traffic from the source network.

Wait interval time

Enter the amount of time in seconds that the Easy VPN Server is to wait for you to generate source traffic. Be sure to give yourself enough time to switch to other systems to generate traffic.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

VPN Troubleshooting: Generate GRE Traffic

This screen appears if you are generating GRE over IPSec traffic.

Have SDM generate VPN Traffic

Select this option if you want Cisco SDM to generate VPN traffic on the interface for debugging.

Enter the remote tunnel IP address

Enter the IP address of the remote GRE tunnel. Do not use the address of the remote interface.

I will generate VPN traffic from the source network

Select this option if you want to generate VPN traffic from the source network.

Wait interval time

Enter the amount of time in seconds that the Easy VPN Server is to wait for you to generate source traffic. Be sure to give yourself enough time to switch to other systems to generate traffic.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

Cisco SDM Warning: SDM will enable router debugs...

This window appears when Cisco SDM is ready to begin advanced troubleshooting. Advanced troubleshooting involves delivering debug commands to the router waiting for results to report, and then removing the debug commands so that router performance is not further affected.

This message is displayed because this process can take several minutes and may affect router performance.

Security Audit

Security Audit is a feature that examines your existing router configurations and then updates your router in order to make your router and network more secure. Security Audit is based on the Cisco IOS AutoSecure feature; it performs checks on and assists in configuration of almost all of the AutoSecure functions. For a complete list of the functions that Security Audit checks for, and for a list of the few AutoSecure features unsupported by Security Audit, see the topic Cisco SDM and Cisco IOS AutoSecure.

Security Audit operates in one of two modes—the Security Audit wizard, which lets you choose which potential security-related configuration changes to implement on your router, and One-Step Lockdown, which automatically makes all recommended security-related configuration changes.

Perform Security Audit

This option starts the Security Audit wizard. The Security Audit wizard tests your router configuration to determine if any potential security problems exist in the configuration, and then presents you with a screen that lets you determine which of those security problems you want to fix. Once determined, the Security Audit wizard will make the necessary changes to the router configuration to fix those problems.

To have Cisco SDM perform a security audit and then fix the problems it has found:

Step 1   In the left frame, select **Security Audit**.

Step 2   Click **Perform Security Audit**.

The Welcome page of the Security Audit wizard appears.

Step 3   Click **Next>**.

The Security Audit Interface Configuration page appears.

Step 4   The Security Audit wizard needs to know which of your router interfaces connect to your inside network and which connect outside of your network. For each interface listed, check either the **Inside** or **Outside** check box to indicate where the interface connects.

Step 5   Click **Next>**.

The Security Audit wizard tests your router configuration to determine which possible security problems may exist. A screen showing the progress of this action appears, listing all of the configuration options being tested for, and whether or not the current router configuration passes those tests.

If you want to save this report to a file, click **Save Report**.

Step 6   Click **Close**.

The Security Audit Report Card screen appears, showing a list of possible security problems.

Step 7   Check the **Fix it** boxes next to any problems that you want Cisco Router and Security Device Manager (Cisco SDM) to fix. For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description to display a help page about that problem.

Step 8   Click **Next>**.

Step 9   The Security Audit wizard may display one or more screens requiring you to enter information to fix certain problems. Enter the information as required and click **Next>** for each of those screens.

Step 10   The Summary page of the wizard shows a list of all the configuration changes that Security Audit will make. Click **Finish** to deliver those changes to your router.

One-Step Lockdown

This option tests you router configuration for any potential security problems and automatically makes any necessary configuration changes to correct any problems found. The conditions checked for and, if needed, corrected are as follows:

- Disable Finger Service

- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Enable Password Encryption Service
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Disable IP Gratuitous ARPs
- Set Minimum Password Length to Less Than 6 Characters
- Set Authentication Failure Rate to Less Than 3 Retries
- Set TCP Synwait Time
- Set Banner
- Enable Logging
- Set Enable Secret Password
- Disable SNMP
- Set Scheduler Interval
- Set Scheduler Allocate
- Set Users
- Enable Telnet Settings
- Enable NetFlow Switching
- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service

- Disable IP Unreachables
- Disable IP Mask Reply
- Disable IP Unreachables on NULL Interface
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces
- Set Access Class on HTTP Server Service
- Set Access Class on VTY Lines
- Enable SSH for Access to the Router

Welcome Page

This screen describes the Security Audit wizard and the changes the wizard will attempt to make to your router configuration.

Interface Selection Page

This screen displays a list of all interfaces and requires you to identify which router interfaces are "outside" interfaces, that is, interfaces that connect to unsecure networks such as the Internet. By identifying which interfaces are outside interfaces, Security Configuration knows on which interfaces to configure firewall security features.

Interface Column

This column lists each of the router interfaces.

Outside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects to a network outside of your network, such as the Internet.

Inside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects directly to your local network and is thus protected from the Internet by your firewall.

Report Card Page

The Report Card popup page displays a list of recommended configuration changes that, if made, make the network more secure. The **Save** button, enabled after all checks are made, lets you save the report card to a file that you can print or email. Clicking **Close** displays a dialog that lists the reported security problems, and that can list security configurations that Cisco SDM can undo.

Fix It Page

This page displays the configuration changes recommended in the Report Card page. Use the **Select an Option** list to display the security problems Cisco SDM can fix, or the security configurations Cisco SDM can undo.

Select an Option: Fix the security problems

The Report Card screen displays a list of recommended configuration changes that will make your router and network more secure. The potential security problems in your router configuration are listed in the left column. To get more information about a potential problem, click the problem. Online help will display a more detailed description of the problem and the recommended configuration changes. To correct all of the potential problems, click **Fix All**, and then click **Next>** to continue. To correct individual security issues, check the **Fix It** check box next to the issue or issues that you want to correct, and then click **Next>** to continue the Security Audit Wizard. The Security Audit will correct the problems you selected, collecting further input from you as necessary, and will then display a list of the new configuration commands that will be added to the router configuration.

Fix All

Click this button to place a check mark next to all of the potential security problems listed on the Report Card screen.

Select an option: Undo Security Configurations

When this option is selected, Cisco SDM displays the security configurations that it can undo. To have Cisco SDM undo all the security configurations, click **Undo All**. To specify a security configuration that you want to undo, check the **Undo** box next to it. **Click Next>** after you have specified which security configurations to undo. You must select at least one security configuration to undo.

Undo All

Click the button to place a checkmark next to all the security configurations that Cisco SDM can undo.

To see which security configurations Cisco SDM can undo, click:

Security Configurations Cisco SDM Can Undo

I want Cisco SDM to fix some problems, but undo other security configurations

If you want Cisco SDM to fix some security issues but undo other security configurations that you do not need, you can run the Security Audit wizard once to specify the problems to fix, and then run it again so that you can select the security configurations you want to undo.

Disable Finger Service

Security Audit disables the finger service whenever possible. Finger is used to find out which users are logged into a network device. Although this information is not usually tremendously sensitive, it can sometimes be useful to an attacker.

In addition, the finger service can be used in a specific type of Denial-of-Service (DoS) attack called "Finger of death," which involves sending a finger request to a specific computer every minute, but never disconnecting.

The configuration that will be delivered to the router to disable the Finger service is as follows:

```
no service finger
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable PAD Service

Security Audit disables all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers whenever possible.

The configuration that will be delivered to the router to disable PAD is as follows:

```
no service pad
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable TCP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their User Datagram Protocol (UDP) versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a Domain Name System (DNS) packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable TCP small servers is as follows:

```
no service tcp-small-servers
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable UDP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their UDP versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable UDP small servers is as follows:

```
no service udp-small-servers
```

Disable IP BOOTP Server Service

Security Audit disables the Bootstrap Protocol (BOOTP) service whenever possible. BOOTP allows both routers and computers to automatically configure necessary Internet information from a centrally maintained server upon startup, including downloading Cisco IOS software. As a result, BOOTP can potentially be used by an attacker to download a copy of a router's Cisco IOS software.

In addition, the BOOTP service is vulnerable to DoS attacks; therefore it should be disabled or filtered via a firewall for this reason as well.

The configuration that will be delivered to the router to disable BOOTP is as follows:

```
no ip bootp server
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Identification Service

Security Audit disables identification support whenever possible. Identification support allows you to query a TCP port for identification. This feature enables an unsecure protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply.

It is dangerous to allow any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable the IP identification service is as follows:

```
no ip identd
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable CDP

Security Audit disables Cisco Discovery Protocol (CDP) whenever possible. CDP is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. This is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable CDP is as follows:

```
no cdp run
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Source Route

Security Audit disables IP source routing whenever possible. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that the datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options.

Disabling IP source routing will cause a Cisco router to never forward an IP packet that carries a source routing option.

The configuration that will be delivered to the router to disable IP source routing is as follows:

```
no ip source-route
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Password Encryption Service

Security Audit enables password encryption whenever possible. Password encryption directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder.

The configuration that will be delivered to the router to enable password encryption is as follows:

```
service password-encryption
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Inbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for inbound Telnet sessions is as follows:

```
service tcp-keepalives-in
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Outbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for outbound Telnet sessions is as follows:

```
service tcp-keepalives-out
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Sequence Numbers and Time Stamps on Debugs

Security Audit enables sequence numbers and time stamps on all debug and log messages whenever possible. Time stamps on debug and log messages indicate the time and date that the message was generated. Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks.

The configuration that will be delivered to the router to enable time stamps and sequence numbers is as follows:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
```

```
service sequence-numbers
```

Enable IP CEF

Security Audit enables Cisco Express Forwarding (CEF) or Distributed Cisco Express Forwarding (DCEF) whenever possible. Because there is no need to build cache entries when traffic starts arriving at new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Routes configured for CEF perform better under SYN attacks than routers using the traditional cache.

The configuration that will be delivered to the router to enable CEF is as follows:

```
ip cef
```

Disable IP Gratuitous ARPs

Security Audit disables IP gratuitous Address Resolution Protocol (ARP) requests whenever possible. A gratuitous ARP is an ARP broadcast in which the source and destination IP addresses are the same. It is used primarily by a host to inform the network about its IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

To disable gratuitous ARPs, the following configuration will be delivered to the router:

```
no ip gratuitous-arps
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Set Minimum Password Length to Less Than 6 Characters

Security Audit configures your router to require a minimum password length of six characters whenever possible. One method attackers use to crack passwords is to try all possible combinations of characters until the password is discovered. Longer passwords have exponentially more possible combinations of characters, making this method of attack much more difficult.

This configuration change will require every password on the router, including the user, enable, secret, console, AUX, tty, and vty passwords, to be at least six characters in length. This configuration change will be made only if the Cisco IOS version running on your router supports the minimum password length feature.

The configuration that will be delivered to the router is as follows:

```
security passwords min-length <6>
```

Set Authentication Failure Rate to Less Than 3 Retries

Security Audit configures your router to lock access after three unsuccessful login attempts whenever possible. One method of cracking passwords, called the "dictionary" attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after three unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the router, this configuration causes a log message to be generated after three unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.

The configuration that will be delivered to the router to lock router access after three unsuccessful login attempts is as follows:

```
security authentication failure rate <3>
```

Set TCP Synwait Time

Security Audit sets the TCP synwait time to 10 seconds whenever possible. The TCP synwait time is a value that is useful in defeating SYN flooding attacks, a form of Denial-of-Service (DoS) attack. A TCP connection requires a three-phase handshake to initially establish the connection. A connection request is sent by the originator, an acknowledgement is sent by the receiver, and then an acceptance of that acknowledgement is sent by the originator. Once this three-phase handshake is complete, the connection is complete and data transfer can begin. A SYN flooding attack sends repeated connection requests to a host, but never sends the acceptance of acknowledgements that complete the connections, creating increasingly more incomplete connections at the host. Because the buffer for incomplete connections is usually smaller than the buffer for completed

connections, this can overwhelm and disable the host. Setting the TCP synwait time to 10 seconds causes the router to shut down an incomplete connection after 10 seconds, preventing the buildup of incomplete connections at the host.

The configuration that will be delivered to the router to set the TCP synwait time to 10 seconds is as follows:

```
ip tcp synwait-time <10>
```

Set Banner

Security Audit configures a text banner whenever possible. In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. The text banner is one method of performing this notification.

The configuration that will be delivered to the router to create a text banner is as follows, replacing *<company name>*, *<administrator email address>*, and *<administrator phone number>* with the appropriate values that you enter into Security Audit:

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Enable Logging

Security Audit will enable logging with time stamps and sequence numbers whenever possible. Because it gives detailed information about network events, logging is critical in recognizing and responding to security events. Time stamps and sequence numbers provide information about the date and time and sequence in which network events occur.

The configuration that will be delivered to the router to enable and configure logging is as follows, replacing *<log buffer size>* and *<logging server ip address>* with the appropriate values that you enter into Security Audit:

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

Set Enable Secret Password

Security Audit will configure the **enable secret** Cisco IOS command for more secure password protection whenever possible. The **enable secret** command is used to set the password that grants privileged administrative access to the Cisco IOS system. The **enable secret** command uses a much more secure encryption algorithm (MD5) to protect that password than the older **enable password** command. This stronger encryption is an essential means of protecting the router password, and thus network access.

The configuration that will be delivered to the router to configure the command is as follows:

```
enable secret <>
```

Disable SNMP

Security Audit disables the Simple Network Management Protocol (SNMP) whenever possible. SNMP is a network protocol that provides a facility for retrieving and posting data about network performance and processes. It is very widely used for router monitoring, and frequently for router configuration changes as well. Version 1 of the SNMP protocol, however, which is the most commonly used, is often a security risk for the following reasons:

- It uses authentication strings (passwords) called *community strings* which are stored and sent across the network in plain text.

- Most SNMP implementations send those strings repeatedly as part of periodic polling.

- It is an easily spoofable, datagram-based transaction protocol.

Because SNMP can be used to retrieve a copy of the network routing table, as well as other sensitive network information, Cisco recommends disabling SNMP if your network does not require it. Security Audit will initially request to disable SNMP.

The configuration that will be delivered to the router to disable SNMP is as follows:

```
no snmp-server
```

Set Scheduler Interval

Security Audit configures the scheduler interval on the router whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. Tuning the scheduler interval ensures that management access to the router is always available by causing the router to run system processes after the specified time interval even when CPU usage is at 100%.

The configuration that will be delivered to the router to tune the scheduler interval is as follows:

```
scheduler interval 500
```

Set Scheduler Allocate

On routers that do not support the command **scheduler interval**, Security Audit configures the **scheduler allocate** command whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. The **scheduler allocate** command guarantees a percentage of the router CPU processes for activities other than network switching, such as management processes.

The configuration that will be delivered to the router to set the scheduler allocate percentage is as follows:

```
scheduler allocate 4000 1000
```

Set Users

Security Audit secures the console, AUX, vty, and tty lines by configuring Telnet user accounts to authenticate access to these lines whenever possible. Security Audit will display a dialog box that lets you define user accounts and passwords for these lines.

Enable Telnet Settings

Security Audit secures the console, AUX, vty, and tty lines by implementing the following configurations whenever possible:

- Configures **transport input** and **transport output** commands to define which protocols can be used to connect to those lines.

- Sets the exec-timeout value to 10 minutes on the console and AUX lines, causing an administrative user to be logged out from these lines after 10 minutes of no activity.

The configuration that will be delivered to the router to secure the console, AUX, vty, and tty lines is as follows:

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Enable NetFlow Switching

Security Audit enables NetFlow switching whenever possible. NetFlow switching is a Cisco IOS feature that enhances routing performance while using Access Control Lists (ACLs) and other features that create and enhance network security.

NetFlow identifies flows of network packets based on the source and destination IP addresses and TCP port numbers. NetFlow then can use just the initial packet of a flow for comparison to ACLs and for other security checks, rather than having to use every packet in the network flow. This enhances performance, allowing you to make use of all of the router security features.

The configuration that will be delivered to the router to enable NetFlow is as follows:

```
ip route-cache flow
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Redirects

Security Audit disables Internet Message Control Protocol (ICMP) redirect messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP redirect messages instruct an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Disabling ICMP redirects will cause no operational impact to the network, and it eliminates this possible method of attack.

The configuration that will be delivered to the router to disable ICMP redirect messages is as follows:

```
no ip redirects
```

Disable IP Proxy ARP

Security Audit disables proxy Address Resolution Protocol (ARP) whenever possible. ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, but a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

The configuration that will be delivered to the router to disable proxy ARP is as follows:

```
no ip proxy-arp
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Directed Broadcast

Security Audit disables IP directed broadcasts whenever possible. An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the extremely common and popular "smurf" Denial-of-Service attack, and they can also be used in related attacks. In a "smurf" attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts causes directed broadcasts that would otherwise be "exploded" into link-layer broadcasts at that interface to be dropped instead.

The configuration that will be delivered to the router to disable IP directed broadcasts is as follows:

```
no ip directed-broadcast
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable MOP Service

Security Audit will disable the Maintenance Operations Protocol (MOP) on all Ethernet interfaces whenever possible. MOP is used to provide configuration information to the router when communicating with DECNet networks. MOP is vulnerable to various attacks.

The configuration that will be delivered to the router to disable the MOP service on Ethernet interfaces is as follows:

```
no mop enabled
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP host unreachable messages is as follows:

```
int <all-interfaces>
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Mask Reply

Security Audit disables Internet Message Control Protocol (ICMP) mask reply messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP mask reply messages are sent when a network devices must know the subnet mask for a particular subnetwork

in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP mask reply messages is as follows:

```
no ip mask-reply
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables on NULL Interface

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. Because the null interface is a packet sink, packets forwarded there will always be discarded and, unless disabled, will generate host unreachable messages. In that case, if the null interface is being used to block a Denial-of-Service attack, these messages flood the local network with these messages. Disabling these messages prevents this situation. In addition, because all blocked packets are forwarded to the null interface, an attacker receiving host unreachable messages could use those messages to determine Access Control List (ACL) configuration.

If the "null 0" interface is configured on your router, Security Audit will deliver the following configuration to the router to disable ICMP host unreachable messages for discarded packets or packets routed to the null interface is as follows:

```
int null 0
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Unicast RPF on Outside Interfaces

Security Audit enables unicast Reverse Path Forwarding (RPF) on all interfaces that connect to the Internet whenever possible. RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

This works only when routing is symmetric. If the network is designed in such a way that traffic from host A to host B may normally take a different path than traffic from host B to host A, the check will always fail, and communication between the two hosts will be impossible. This sort of asymmetric routing is common in the Internet core. Ensure that your network does not use asymmetric routing before enabling this feature.

In addition, unicast RPF can be enabled only when IP Cisco Express Forwarding (CEF) is enabled. Security Audit will check the router configuration to see if IP CEF is enabled. If IP CEF is not enabled, Security Audit will recommend that IP CEF be enabled and will enable it if the recommendation is approved. If IP CEF is not enabled, by Security Audit or otherwise, unicast RPF will not be enabled.

To enable unicast RPF, the following configuration will be delivered to the router for each interface that connects outside of the private network, replacing *<outside interface>* with the interface identifier:

```
interface <outside interface>
ip verify unicast reverse-path
```

Enable Firewall on All of the Outside Interfaces

If the Cisco IOS image running on the router includes the Firewall feature set, then Security Audit will enable Context-Based Access Control (CBAC) on the router whenever possible. CBAC, a component of the Cisco IOS Firewall feature set, filters packets based on application-layer information, such as what kinds of commands are being executed within the session. For example, if a command that is not supported is discovered in a session, the packet can be denied access.

CBAC enhances security for TCP and User Datagram Protocol (UDP) applications that use well-known ports, such as port 80 for HTTP or port 443 for Secure Sockets Layer (SSL). It does this by scrutinizing source and destination

addresses. Without CBAC, advanced application traffic is permitted only by writing Access Control Lists (ACLs). This approach leaves firewall doors open, so most administrators tend to deny all such application traffic. With CBAC enabled, however, you can securely permit multimedia and other application traffic by opening the firewall as needed and closing it all other times.

To enable CBAC, Security Audit will use Cisco SDM's Create Firewall screens to generate a firewall configuration.

Set Access Class on HTTP Server Service

Security Audit enables the HTTP service on the router with an access class whenever possible. The HTTP service permits remote configuration and monitoring using a web browser, but is limited in its security because it sends a clear-text password over the network during the authentication process. Security Audit therefore limits access to the HTTP service by configuring an access class that permits access only from directly connected network nodes.

The configuration that will be delivered to the router to enable the HTTP service with an access class is as follows:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Set Access Class on VTY Lines

Security Audit configures an access class for vty lines whenever possible. Because vty connections permit remote access to your router, they should be limited only to known network nodes.

The configuration that will be delivered to the router to configure an access class for vty lines is as follows:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

In addition, the following configuration will be applied to each vty line:

```
access-class <std-acl-num>
```

Enable SSH for Access to the Router

If the Cisco IOS image running on the router is a crypto image (an image that uses 56-bit Data Encryption Standard (DES) encryption and is subject to export restrictions), then Security Audit will implement the following configurations to secure Telnet access whenever possible:

- Enable Secure Shell (SSH) for Telnet access. SSH makes Telnet access much more secure.

- Set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds.

- Set the maximum number of unsuccessful SSH login attempts to two before locking access to the router.

The configuration that will be delivered to the router to secure access and file transfer functions is as follows:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

> **Note**   After making the configuration changes above, you must specify the SSH modulus key size and generate a key. Use the SSH page to do so.

Enable AAA

Cisco IOS Authentication, Authorization, and Accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco SDM will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router:

- Configure authentication and authorization for VTY lines

    The local database will be used for both authentication and authorization.

- Configure authentication for a console line

    The local database will be used for authentication.

- Modify HTTP authentication to use the local database

Configuration Summary Screen

This screen displays a list of all the configuration changes that will be delivered to the router configuration, based on the security problems that you selected to fix in the Report Card screen.

Cisco SDM and Cisco IOS AutoSecure

AutoSecure is a Cisco IOS feature that, like Cisco SDM, lets you more easily configure security features on your router, so that your network is better protected. Cisco SDM implements almost all of the configurations that AutoSecure affords.

AutoSecure Features Implemented in Cisco SDM

The following AutoSecure features are implemented in this version of Cisco SDM. For an explanation of these services and features, click the links below:

- Disable SNMP
- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route

- Disable IP Redirects

- Disable IP Proxy ARP

- Disable IP Directed Broadcast

- Disable MOP Service

- Disable IP Unreachables

- Disable IP Unreachables on NULL Interface

- Disable IP Mask Reply

- Enable Password Encryption Service

- Disable IP Unreachables on NULL Interface

- Disable IP Unreachables on NULL Interface

- Set Minimum Password Length to Less Than 6 Characters

- Enable IP CEF

- Enable Firewall on All of the Outside Interfaces

- Set Users

- Enable Logging

- Enable Firewall on All of the Outside Interfaces

- Set Minimum Password Length to Less Than 6 Characters

- Enable Firewall on All of the Outside Interfaces

- Set Users

- Set Users

- Set Users

- Enable Unicast RPF on Outside Interfaces

- Enable Firewall on All of the Outside Interfaces

AutoSecure Features Not Implemented in Cisco SDM

The following AutoSecure features are not implemented in this version of Cisco SDM:

- Disabling NTP—Based on input, AutoSecure will disable the Network Time Protocol (NTP) if it is not necessary. Otherwise, NTP will be configured with MD5 authentication. Cisco SDM does not support disabling NTP.

- Configuring AAA—If the Authentication, Authorization, and Accounting (AAA) service is not configured, AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. Cisco SDM does not support AAA configuration.

- Setting SPD Values—Cisco SDM does not set Selective Packet Discard (SPD) values.

- Enabling TCP Intercepts—Cisco SDM does not enable TCP intercepts.

- Configuring anti-spoofing ACLs on outside interfaces—AutoSecure creates three named access lists used to prevent anti-spoofing source addresses. Cisco SDM does not configure these ACLs.

AutoSecure Features Implemented Differently in Cisco SDM

- Disable SNMP—Cisco SDM will disable SNMP, but unlike AutoSecure, it does not provide an option for configuring SNMP version 3.

- Enable SSH for Access to the Router—Cisco SDM will enable and configure SSH on crypto Cisco IOS images, but unlike AutoSecure, it will not enable Service Control Point (SCP) or disable other access and file transfer services, such as FTP.

Security Configurations Cisco SDM Can Undo

This table lists the security configurations that Cisco SDM can undo.

Security Configuration	Equivalent CLI
Disable Finger Service	No service finger
Disable PAD Service	No service pad
Disable TCP Small Servers Service	No service tcp-small-servers no service udp-small-servers
Disable IP BOOTP Server Service	No ip bootp server
Disable IP Identification Service	No ip identd
Disable CDP	No cdp run
Disable IP Source Route	No ip source-route

Security Configuration	Equivalent CLI
Enable NetFlow Switching	ip route-cache flow
Disable IP Redirects	no ip redirects
Disable IP Proxy ARP	no ip proxy-arp
Disable IP Directed Broadcast	no ip directed-broadcast
Disable MOP Service	No mop enabled
Disable IP Unreachables	int <all-interfaces>
	no ip unreachables
Disable IP Mask Reply	no ip mask-reply
Disable IP Unreachables on NULL Interface	int null 0
	no ip unreachables
Enable Password Encryption Service	service password-encryption
Enable TCP Keepalives for Inbound Telnet Sessions	service tcp-keepalives-in
Enable TCP Keepalives for Outbound Telnet Sessions	service tcp-keepalives-out
Disable IP Gratuitous ARPs	no ip gratuitous arps

Undoing Security Audit Fixes

Cisco SDM can undo this security fix. If you want Cisco SDM to remove this security configuration, run the Security Audit wizard. In the Report Card window, select the option **Undo Security Configurations**, place a check mark next to this configuration and other configurations that you want to undo, and click **Next>**.

Add or Edit Telnet/SSH Account Screen

This screen lets you add a new user account or edit an existing user account for Telnet and SSH access to your router.

User Name

Enter the username for the new account in this field.

Password

Enter the password for the new account in this field.

Confirm Password

Reenter the new account password in this field for confirmation. The entry in this field must match the entry in the password field.

Configure User Accounts for Telnet/SSH Page

This screen lets you manage the user accounts that have Telnet or Secure Shell (SSH) access to your router. The table in this screen shows each Telnet user account, listing the account username and displaying asterisks to represent the account password. Note that this screen appears only if you have not already configured any user accounts; therefore, the table on this screen is always empty when it is initially displayed.

Enable Authorization for Telnet Check Box

Check this box to enable Telnet and SSH access to your router. Clear this box to disable Telnet and SSH access to your router.

Add... Button

Click this button to display the Add a User Account screen, letting you add an account by assigning the account a username and password.

Edit... Button

Click a user account in the table to select it, and click this button to display the Edit a User Account screen, letting you edit the username and password of the selected account.

Delete Button

Click a user account in the table to select it, and click this button to delete the selected account.

Enable Secret and Banner Page

This screen lets you enter a new enable secret and a text banner for the router.

The enable secret is an encrypted password that provides administrator-level access to all functions of the router. It is vital that the secret be secure and difficult to crack. Your secret must be a minimum of six characters long, and it is recommended that you include both alphabetic and numeric characters and that you do not use a word that can be found in a dictionary, or that might be personal information about yourself that someone might be able to guess.

The text banner will be displayed whenever anyone connects to your router using Telnet or SSH. The text banner is an important security consideration because it is a method of notifying unauthorized individuals that access to your router is prohibited. in some jurisdictions, this is a requirement for civil and/or criminal prosecution.

New Password

Enter the new enable secret in this field.

Re-enter New Password

Re-enter the new enable secret in this field for verification.

Login Banner

Enter the text banner that you want configured on your router.

Logging Page

This screen lets you configure the router log by creating a list of syslog servers where log messages will be forwarded, and by setting the logging level, which determines the minimum severity a log message must have in order for it to be captured.

IP Address/Hostname Table

This table displays a list of hosts to where the router log messages will be forwarded. These hosts should be syslog servers that can trap and manage the router log messages.

Add... Button

Click this button to display the IP Address/Host Name screen, letting you add a syslog server to the list by entering either its IP address or host name.

Edit... Button

Click a syslog server in the table to select it, and click this button to display the IP Address/Host Name screen, letting you edit the IP address or host name of the selected syslog server.

Delete Button

Click a syslog server in the table to select it, and click this button to delete the selected syslog server from the table.

Set logging level Field

In this field, select the minimum severity level that a router log message must have in order for it to be trapped and forwarded to the syslog server(s) in the table on this screen. A log message severity level is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

- 0 - emergencies

  System unusable
- 1- alerts

Immediate action needed

– 2 - critical

Critical conditions

– 3 - errors

Error conditions

– 4 - warnings

Warning conditions

– 5 - notifications

Normal but significant condition

– 6 - informational

Informational messages only

– 7 - debugging

Debugging messages

Routing

The Routing window displays the configured static routes and Routing Internet Protocol, (RIP), Open Shortest Path First (OSPF), and Extended Interior Gateway Routing Protocol (EIGRP) configured routes. From this window, you can review the routes, add new routes, edit existing routes, and delete routes.

Note Static and dynamic routes configured for GRE over IPSec tunnels will appear in this window. If you delete a routing entry that is used for GRE over IPSec tunneling in this window, that route will no longer be available to the tunnel.

Static Routing

Destination Network

This is the network that the static route provides a path to.

Forwarding

This is the interface or IP address through which packets must be sent to reach the destination network.

Optional

This area shows whether a distance metric has been entered, and whether or not the route has been designated as a permanent route.

What Do You Want To Do?

If you want to:	Do this:
Add a static route.	Click **Add**, and create the static route in the Add a Static Route window.
Edit a static route.	Select the static route, and click **Edit**. Edit the route information in the IP Static Route window. When a route has been configured that SDM does not support, the Edit button is disabled.
Delete a static route.	Select the static route, and click **Delete**. Then, confirm the deletion in the warning window.
Delete all static routes.	Click **Delete All**. Then, confirm the deletion in the warning window.

Note
- If SDM detects a previously configured static route entry that has the next hop interface configured as the "Null" interface, then the static route entry will be read-only.
- If SDM detects a previously configured static route entry with "tag" or "name" options, that entry will be read-only.
- If you are configuring a Cisco 7000 router, and the interface used for a next hop is unsupported, that route will be marked as read only.
- Read-only entries cannot be edited or deleted using SDM.

Dynamic Routing

This portion of the window allows you to configure RIP, OSPF, and EIGRP dynamic routes.

Item Name

If no dynamic routes have been configured, this column contains the text RIP, OSPF, and EIGRP. When one or more routes have been configured, this column contains the parameter names for the type of routing configured.

Routing Protocol	Configuration Parameters
RIP	RIP Version, Network, Passive Interface
OSPF	Process ID
EIGRP	Autonomous System Number

Item Value

This column contains the text "Enabled," and configuration values when a routing type has been configured. It contains the text "Disabled" when a routing protocol has not been configured.

What Do You Want To Do?

If you want to:	Do this:
Configure an RIP route.	Select the RIP tab and click **Edit**. Then, configure the route in the RIP Dynamic Route window.
Configure an OSPF route.	Select the OSPF tab and click **Edit**. Then, configure the route in the displayed window.
Configure an EIGRP route.	Select the EIGRP tab and click **Edit**. Then, configure the route in the displayed window.

Add or Edit IP Static Route

Use this window to add or edit a static route.

Destination Network

Enter the destination network address information in these fields.

Prefix

Enter the IP address of the destination network. For more information, refer to Available Interface Configurations.

Prefix Mask

Enter the destination address subnet mask.

Make this the default route

Check this box to make this the default route for this router. A default route forwards all the unknown outbound packets through this route.

Forwarding

Specify how to forward data to the destination network.

Interface

Click **Interface** if you want to select the interface of the router that forwards the packet to the remote network.

IP Address

Click **IP Address** if you want to enter the IP Address of the next hop router that receives and forwards the packet to the remote network.

Optional

You can optionally provide a distance metric for this route, and designate it as a permanent route.

Distance Metric for this route

Enter the metric value that has to be entered in the routing table. Valid values are 1 through 255.

Permanent Route

Check this box to make this static route entry a permanent route. Permanent routes are not deleted even if the interface is shut down or the router is unable to communicate with the next router.

Add or Edit an RIP Route

Use this window to add or edit a Routing Internet Protocol (RIP) route.

RIP Version

The values are RIP version 1, RIP version 2, and Default. Select the version supported by the Cisco IOS image that the router is running. When you select version 1, the router sends version 1 RIP packets and can receive version 1 packets. When you select version 2, the router sends version 2 RIP packets and can receive version 2 packets. When you select Default, the router sends version 1 packets, and can receive both version 1 and version 2 RIP packets.

IP Network List

Enter the networks on which you want to enable RIP. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will still receive routing updates, however.

Add or Edit an OSPF Route

Use this window to add or edit an Open Shortest Path First (OSPF) route.

OSPF Process ID

This field is editable when OSPF is first enabled; it is disabled once OSPF routing has been enabled. The process ID identifies the router's OSPF routing process to other routers.

IP Network List

Enter the networks that you want to create routes to. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Network

The address of the destination network for this route. For more information, refer to Available Interface Configurations.

Mask

The subnet mask used on that network.

Area

The OSPF area number for that network. Each router in a particular OSPF area maintains a topological database for that area.

Note If SDM detects previously configured OSPF routing that includes "area" commands, then the IP Network List table will be read-only and cannot be edited.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will still receive routing updates, however.

Add

Click **Add** to provide an IP address, network mask, and area number in the IP address window.

Edit

Click **Edit** to edit the IP address, network mask, or area number in the IP address window.

Add or Edit EIGRP Route

Use this window to add or delete an Extended IGRP (EIGRP) route.

Autonomous System Number

The autonomous system number is used to identify the router's EIGRP routing process to other routers.

IP Network List

Enter the networks that you want to create routes to. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will neither send nor receive routing updates.

⚠️

Caution   When you make an interface passive, EIGRP suppresses the exchange of hello packets between routers, resulting in the loss of their neighbor relationship. This not only stops routing updates from being advertised, but also suppresses incoming routing updates.

Add

Click **Add** to add a destination network IP address to the Network list.

Delete

Select an IP address, and click **Delete to remove an IP address** from the Network list.

Add or Edit EIGRP Route

Network Address Translation

Network Address Translation (NAT) is a robust form of address translation that extends addressing capabilities by providing both static address translations and dynamic address translations. NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet. The hosts may be using private addresses or addresses assigned to another organization; in either case, NAT allows these addresses that are not Internet-ready to continue to be used but still allow communication with hosts across the Internet.

Network Address Translation Wizards

You can use a wizard to guide you in creating a Network Address Translation (NAT) rule. Choose one of the following wizards:

- Basic NAT

    Choose the Basic NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts but no servers. Look at the sample diagram that appears to the right when you choose **Basic NAT**. If your network is made up only of PCs that require access to the Internet, choose **Basic NAT** and click the **Launch** button.

- Advanced NAT

    Choose the Advanced NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts and servers, *and* the servers must be accessible to outside hosts (hosts on the Internet). Look at the sample diagram that appears to the right when you choose **Advanced NAT**.

If your network has e-mail servers, web servers, or other types of servers and you want them to accept connections from the Internet, choose **Advanced NAT** and click the **Launch** button.

✎
Note   If you do not want your servers to accept connections from the Internet, you can use the Basic NAT wizard.

Basic NAT Wizard: Welcome

The Basic NAT welcome window shows how the wizard will guide you through configuring NAT for connecting one or more LANs, but no servers, to the Internet.

Basic NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

✎
Note   Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface
- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

Note   If Cisco SDM detects a conflict between the NAT configuration and an existing VPN configuration for the WAN interface, it will inform you with a dialog box after you click **Next**.

Summary

This window shows you the NAT configuration you created, and allows you to save the configuration. The summary will appear similar to the following:

```
Interface that is connected to the Internet or to your Internet
service provider:
    FastEthernet0/0

IP address ranges that share the Internet connection:
    108.1.1.0 to 108.1.1.255
    87.1.1.0 to 87.1.1.255
    12.1.1.0 to 12.1.1.255
    10.20.20.0 to 10.20.20.255
```

If you used the Advanced NAT wizard, you may also see additional information similar to the following:

```
NAT rules for servers:
    Translate 10.10.10.19 TCP port 6080 to IP address of interface
FastEthernet0/0 TCP port 80
    Translate 10.10.10.20 TCP port 25 to 194.23.8.1 TCP port 25
```

Advanced NAT Wizard: Welcome

The Advanced NAT welcome window shows how the wizard will guide you through configuring NAT for connecting your LANs and servers to the Internet.

Advanced NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Additional Public IP Addresses

Click **Add** to enter public IP addresses that you own. You will be able to assign these IP address to servers on your network that you want to make available to the Internet.

To delete an IP address from the list, choose the IP address and click **Delete**.

Add IP Address

Enter a public IP address that you own. You will be able to assign this IP address to a server on your network that you want to make available to the Internet.

Advanced NAT Wizard: Networks

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

Note Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface

- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

To add a network not directly connected to your router to the list, click **Add Networks**.

✎

Note   If Cisco SDM does not allow you to place a check mark next to a network for which you want to configure a NAT rule, the interface associated with the network has already been designated as a NAT interface. This status will be indicated by the word *Designated* in the Comments column. If you want to configure a NAT rule for that interface, exit the wizard, click the **Edit NAT** tab, click **Designate NAT Interfaces**, and uncheck the interface. Then return to the wizard and configure the NAT rule.

Add Network

You can add a network to the list of networks made available in the Advanced NAT wizard. You must have the network IP address and network mask. For more information, see IP Addresses and Subnet Masks.

IP Address

Enter the network IP address.

Subnet Mask

Enter the network subnet mask in this field, or choose the number of subnet bits from the scrolling field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Advanced NAT Wizard: Server Public IP Addresses

This window allows you to translate public IP addresses to the private IP addresses of internal servers that you want to make accessible from the Internet.

The list shows the private IP addresses and ports (if used) and the public IP addresses and ports (if used) to which they are translated.

To reorder the list based on the private IP addresses, click the column head **Private IP Address**. To reorder the list based on the public IP addresses, click the column head **Public IP Address**.

Add Button

To add a translation rule for a server, click **Add**.

Edit Button

To edit a translation rule for a server, choose it in the list and click **Edit**.

Delete Button

To delete a translation rule, choose it in the list and click **Delete**.

Add or Edit Address Translation Rule

In this window you can enter or edit the IP address translation information for a server.

Private IP Address

Enter the IP address that the server uses on your internal network. This is an IP address that cannot be used externally on the Internet.

Public IP Address

From the drop-down menu, choose the public IP address to which the server's private IP address will be translated. The IP addresses that appear in the drop-down menu include the IP address of the router WAN interface and any public IP addresses you own that were entered in the connections window (see Advanced NAT Wizard: Connection).

Type of Server

Choose one of the following server types from the drop-down menu:

- Web server

  An HTTP host serving HTML and other WWW-oriented pages.

- E-mail server

  An SMTP server for sending Internet mail.

- Other

  A server which is not a web or e-mail server, but which requires port translation to provide service. This choice activates the Translated Port field and the Protocol drop-down menu.

If you do not choose a server type, all traffic intended for the public IP address you choose for the server will be routed to that address, and no port translation will be done.

Original Port

Enter the port number used by the server to accept service requests from the internal network.

Translated Port

Enter the port number used by the server to accept service requests from the Internet.

Protocol

Choose **TCP** or **UDP** for the protocol used by the server with the original and translated ports.

Advanced NAT Wizard: ACL Conflict

If this window appears, Cisco SDM has detected a conflict between the NAT configuration and an existing ACL on the WAN interface. This ACL may be part of a firewall configuration, a VPN configuration, or the configuration of another feature.

Choose to modify the NAT configuration to remove the conflict, or choose to *not* modify the NAT configuration. If you choose to *not* modify the NAT configuration, the conflict may cause other features you have configured to stop working.

View Details

Click the **View Details** button to see the proposed modifications to the NAT configuration to resolve the conflict. This button is not displayed with all feature conflicts.

Details

This window lists the changes Cisco SDM will make to the NAT configuration to resolve conflicts between NAT and another feature configured on the same interface.

Network Address Translation Rules

The Network Address Translation Rules window lets you view NAT rules, view address pools, and set translation timeouts. From this window you can also designate interfaces as inside or outside interfaces.

For more information on NAT, follow the link More About NAT.

Designate NAT Interfaces

Click to designate interfaces as inside or outside. NAT uses the inside/outside designations as reference points when interpreting translation rules. Inside interfaces are those interfaces connected to the private networks that the router serves. Outside interfaces connect to the WAN or to the Internet. The designated inside and outside interfaces are listed above the NAT rule list.

Address Pools

Click this button to configure or edit address pools. Address pools are used with dynamic address translation. The router can dynamically assign addresses from the pool as they are needed. When an address is no longer needed, it is returned to the pool.

Translation Timeouts

When dynamic NAT is configured, translation entries have a timeout period after which they expire and are purged from the translation table. Click this button to configure the timeout values for NAT translation entries and other values.

Network Address Translation Rules

This area shows the designated inside and outside interfaces and the NAT rules that have been configured.

Inside Interfaces

The inside interfaces are the interfaces that connect to the private networks the router serves. NAT uses the inside designation when interpreting a NAT translation rule. You can designate interfaces as inside by clicking **Designate NAT interfaces**.

Outside Interfaces

The outside interfaces are the router interfaces that connect to the WAN or the Internet. NAT uses the outside designation when interpreting a NAT translation rule. You can designate interfaces as outside by clicking **Designate NAT interfaces**.

Original Address

This is the private address or set of addresses that is used on the LAN.

Translated Address

This is the legal address or range of addresses that is used on the Internet or the external network.

Rule Type

Rules are either static address translation rules or dynamic address translation rules.

Static address translation allows hosts with private addresses to access the Internet and to be publicly accessible from the Internet. It statically maps one private IP address to one public or global address. If you wanted to provide static translation to ten private addresses, you would create a separate static rule for each address.

Dynamic address translation. There are two methods of dynamic addressing using NAT. One method maps multiple private addresses to a single public address and the port numbers of host sessions to determine which host to route returning traffic to. The second method uses named address pools. These address pools contain public addresses. When a host with a private address needs to establish communication outside the LAN, it is given a public address from this pool. When the host no longer needs it, the address is returned to the pool.

Clone selected entry on Add

If you want to use an existing rule as the basis for a new rule that you want to create, choose the rule and check this check box. When you click **Add**, the addresses in the rule you chose appear in the Add Address Translation Rule window. You can edit these addresses to obtain the ones you need for the new rule instead of entering the entire address into each field.

What Do You Want to Do?

If you want to:	Do this:
Designate the inside and outside interfaces. You must designate at least one inside interface and one outside interface in order for the router to perform NAT.	Click **Designate NAT interfaces**, and designate interfaces as inside or outside in the NAT Interface Setting window. Interfaces can also be designated as inside or outside interfaces in the Interfaces and Connections window.
Add, edit, or delete an address pool. Dynamic rules can use address pools to assign addresses to devices as they are needed.	Click **Address Pools**, and configure address pool information in the dialog box.
Set the translation timeout.	Click **Translation Timeouts**, and set the timeout in the Translation Timeouts window.
Add a NAT rule.	Click **Add**, and create the NAT rule in the Add Address Translation Rule window. If you want to use an existing NAT rule as a template for the new rule, choose the rule, click **Clone selected entry on Add**, and then click **Add**.

If you want to:	Do this:
Edit a NAT rule.	Choose the NAT rule that you want to edit, click **Edit**, and edit the rule in the Edit Address Translation Rule window.
Delete a NAT rule.	Choose the NAT rule that you want to delete, and click **Delete**. You must confirm deletion of the rule in the Warning box displayed.
View or edit route maps. If virtual private network (VPN) connections are configured on the router, the local IP addresses in the VPN must be protected from NAT translations. When both a VPN and NAT are configured, Cisco Router and Security Device Manager (Cisco SDM) creates route maps to protect IP addresses in a VPN from being translated. Additionally, route maps can be configured using the command-line interface (CLI). You can view configured route maps and edit the access rule they use.	Click **View Route MAP**.
Find out how to perform related configuration tasks.	See one of the following procedures: • How Do I Configure NAT Passthrough for a VPN? • How Do I Configure NAT on an Unsupported Interface? • How Do I Configure NAT Passthrough for a Firewall?

Note   Many conditions cause previously configured NAT rules to appear as read-only in the Network Address Translation Rules list. Read-only NAT rules are not editable. For more information, see the help topic Reasons that Cisco SDM Cannot Edit a NAT Rule.

Designate NAT Interfaces

Use this window to designate the inside and outside interfaces that you want to use in NAT translations. NAT uses the inside and outside designations when interpreting translation rules, because translations are performed from inside to outside, or from outside to inside.

Once designated, these interfaces are used in all NAT translation rules. The designated interfaces appear above the Translation Rules list in the main NAT window.

Interface

All router interfaces are listed in this column.

Inside (trusted)

Check to designate an interface as an inside interface. Inside interfaces typically connect to a LAN that the router serves.

Outside (untrusted)

Check to designate an interface as an outside interface. Outside interfaces typically connect to your organization's WAN or to the Internet.

Translation Timeout Settings

When you configure dynamic NAT translation rules, translation entries have a timeout period after which they expire and are purged from the translation table. Set the timeout values for various translations in this window.

DNS Timeout

Enter the number of seconds after which connections to DNS servers time out.

ICMP Timeout

Enter the number of seconds after which Internet Control Message Protocol (ICMP) flows time out. The default is 60 seconds.

PPTP Timeout

Enter the number of seconds after which NAT Point-to-Point Tunneling Protocol (PPTP) flows time out. The default is 86400 seconds (24 hours).

Dynamic NAT Timeout

Enter the maximum number of seconds that dynamic NAT translations should live.

Max Number of NAT Entries

Enter the maximum number of NAT entries in the translation table.

UDP flow timeouts

Enter the number of seconds that translations for User Datagram Protocol (UDP) flows should live. The default is 300 seconds (5 minutes).

TCP flow timeouts

Enter the number of seconds that translations for Transmission Control Protocol (TCP) flows should live. The default is 86400 seconds (24 hours).

Reset Button

Clicking this button resets translation and timeout parameters to their default values.

Edit Route Map

When VPNs and NAT are both configured on a router, packets that would normally meet the criteria for an IPSec rule will not do so if NAT translates their IP addresses. In this case, NAT translation will cause packets to be sent without being encrypted. Cisco SDM may create route maps to prevent NAT from translating IP addresses that you want to be preserved.

Although Cisco SDM only creates route maps to limit the action of NAT, route maps can be used for other purposes as well. If route maps have been created using the CLI, they will be visible in this window as well.

Name

The name of this route map.

Route map entries

This box lists the route map entries.

Name
The name of the route map entry.

Seq No.
The sequence number of the route map.

Action
Route maps created by Cisco SDM are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists
The access lists that specify the traffic to which this route map applies.

To Edit a Route Map Entry

Choose the entry, click **Edit**, and edit the entry in the Edit Route Map Entry window.

Edit Route Map Entry

Use this window to edit the access list specified in a route map entry.

Name

A read-only field containing the name of the route map entry.

Seq No.

A read-only field containing the sequence number for the route map. When Cisco SDM creates a route map, it automatically assigns it a sequence number.

Action

Either **permit** or **deny**. Route maps created by Cisco SDM are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists

This area shows the access lists associated with this entry. The route map uses these access lists to determine which traffic to protect from NAT translation.

To Edit an Access List in a Route Map Entry

Choose the access list, and click **Edit**. Then edit the access list in the windows displayed.

Address Pools

The Address Pools window shows the configured address pools that can be used in dynamic NAT translation.

Pool Name

This field contains the name of the address pool. Use this name to refer to the pool when configuring a dynamic NAT rule.

Address

This field contains the IP address range in the pool. Devices whose IP addresses match the access rule specified in the Add Address Translation Rule window will be given private IP addresses from this pool.

What Do You Want to Do?

If you want to:	Do this:
Add an address pool to the router configuration.	Click **Add**, and configure the pool in the Add Address Pool window.
	If you want to use an existing pool as a template for the new pool, choose the existing pool, check **Clone selected entry on Add**, and click **Add**.
Edit an existing address pool.	Choose the pool entry, click **Edit**, and edit the pool configuration in the Edit Address Pool window.
Delete an address pool.	Choose the pool entry, click **Delete**, and confirm deletion in the Warning box displayed.

> **Note**   If Cisco SDM detects a previously configured NAT address pool that uses the "type" keyword, that address pool will be read-only and cannot be edited.

Add or Edit Address Pool

Use this window to specify an address pool for dynamic address translation, an address for Port Address Translation (PAT), or a TCP load-balancing rotary pool.

Pool Name

Enter the name of the address pool.

Port Address Translation (PAT)

There may be times when most of the addresses in the pool have been assigned, and the IP address pool is nearly depleted. When this occurs, PAT can be used with a single IP address to satisfy additional requests for IP addresses. Check this check box if you want the router to use PAT when the address pool is close to depletion.

IP Address

Enter the lowest-numbered IP address in the range in the left field; enter the highest-numbered IP address in the range in the right field. For more information, see Available Interface Configurations.

Network Mask

Enter the subnet mask or the number of network bits that specify how many bits in the IP addresses are network bits.

Add or Edit Static Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

✎

Note   If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco SDM or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

This help topic describes how to use the Add Address Translation Rule fields when **From inside to outside** is chosen.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal addresses on the Internet or on your organization's intranet. You may want to choose this option if you use private addresses on your LAN that are not globally unique on the Internet.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area lists the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the address of a single host and a translated address, known as the *inside global address*, enter the IP address for that host. Do not enter a subnet mask in the Network Mask field.

- If you want to create *n*-to-*n* mappings between the private addresses in a subnet to corresponding inside global addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco SDM to translate the addresses of a subnet, enter the mask for that subnet. Cisco SDM determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

• Choose **IP Address** if you want the address to be translated to the address defined in the IP Address field.

• Choose **Interface** if you want the *Translate from* address to use the address of an interface on the router. The *Translate from* address will be translated to the IP address assigned to the interface that you specify in the Interface field.

Interface

This field is enabled if Interface is chosen in the Type field. This field lists the interfaces on the router. Choose the interface whose IP address you want the local inside address translated to.

> **Note** If **Interface** is chosen in the Type field, only translations that redirect TCP/IP ports are supported. The Redirect Port check box is automatically checked and cannot be unchecked.

IP Address

This field is enabled if you chose **IP Address** in the Type field. Do one of the following:

• If you are creating a one-to-one mapping between a single inside local address and a single inside global address, enter the inside global address in this field.

• If you are mapping the inside local addresses of a subnet to the corresponding inside global addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the *Translate from* Interface area will be used to calculate the remaining inside global addresses.

> ✎
>
> **Note** If you do not enter a network mask in the Translate from Interface area, Cisco SDM will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the inside device in the translation. This enables you to use the same public IP address for multiple devices, as long as the port specified for each device is different. You must create an entry for each port mapping for this "Translated to" address.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the inside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Static Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, then the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

> ✎
>
> **Note** If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate

addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco SDM or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you choose **From outside to inside**, this area contains the designated outside interfaces.

> ✎
>
> **Note**   If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the outside global address of a single remote host and a translated address, known as the *outside local address*, enter the IP address for the remote host.

- If you want to create *n*-to-*n* mappings between the addresses in a remote subnet to corresponding outside local addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco SDM to translate the addresses in a remote subnet, enter the mask for that subnet. Cisco SDM determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

IP Address

Do one of the following:

- If you are creating a one-to-one mapping between a single outside global address and a single outside local address, enter the outside local address in this field.

- If you are mapping the outside global addresses of a remote subnet to the corresponding outside local addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the Translate from Interface area will be used to calculate the remaining outside local addresses.

Note If you do not enter a network mask in the Translate from Interface area, Cisco SDM will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the outside device in the translation. This enables you to use extended static translation and to use the same public IP address for multiple devices, as long as the port specified for each device is different.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the outside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal (globally unique) addresses on the Internet or on your organization's intranet.

This help topic describes how the remaining fields are used when From inside to outside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From inside to outside**, these are the inside local addresses. Enter the name or number of the access rule that defines the addresses

you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose **Address Pool** in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note   If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco SDM will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you chose **From outside to inside**, this area contains the designated outside interfaces.

> **Note**   If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From outside to inside**, these are the outside global addresses. Enter the name or number of the access rule that defines the addresses you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose Address Pool in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

How Do I . . .

This section contains procedures for tasks that the wizard does not help you complete.

How do I Configure Address Translation for Outside to Inside

The NAT wizard allows you to configure a Network Address Translation (NAT) rule to translate addresses from inside to outside. To configure a NAT rule to translate addresses from outside to inside, follow the directions in one of the following sections:

- Add or Edit Dynamic Address Translation Rule: Outside to Inside
- Add or Edit Static Address Translation Rule: Outside to Inside

How Do I Configure NAT With One LAN and Multiple WANs?

The NAT wizard allows you to configure a Network Address Translation (NAT) rule between one LAN interface on your router and one WAN interface. If you want to configure NAT between one LAN interface on your router and multiple WAN interfaces, first use the NAT wizard to configure an address translation rule between the LAN interface on your router and one WAN interface. Then follow the directions in one of the following sections:

- Add or Edit Static Address Translation Rule: Inside to Outside
- Add or Edit Dynamic Address Translation Rule: Inside to Outside

Each time you add a new address translation rule using the directions in one of these sections, choose the same LAN interface and a new WAN interface. Repeat this procedure for all WAN interfaces that you want to configure with address translation rules.

How Do I . . .

C H A P T E R 27

Cisco IOS IPS

The Cisco IOS Intrusion Prevention System (Cisco IOS IPS) allows you to manage intrusion prevention on routers that use Cisco IOS Release 12.3(8)T4 or later releases. Cisco IOS IPS lets you monitor and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.

Cisco SDM lets you control the application of Cisco IOS IPS on interfaces, import and edit signature definition files (SDF) from Cisco.com, and configure the action that Cisco IOS IPS is to take if a threat is detected.

IPS Tabs

Use the tabs at the top of the IPS window to go to the area where you need to work.

- Create IPS—Click to go to the IPS Rule wizard to create a new Cisco IOS IPS rule.

- Edit IPS—Click to edit Cisco IOS IPS rules and apply or remove them from interfaces.

- Security Dashboard—Click to view the Top Threats table and deploy signatures associated with those threats.

- IPS Migration—If the router runs a Cisco IOS image of release 12.4(11)T or later, you can migrate Cisco IOS IPS configurations created using earlier versions of the Cisco IOS.

IPS Rules

A Cisco IOS IPS rule specifies an interface, the type and direction of traffic that it is to examine, and the location of the signature definition file (SDF) that the router uses.

Create IPS

In this window you can launch the IPS Rule wizard.

The IPS Rule wizard prompts you for the following information:

- The interface on which to apply the rule
- The traffic on which to apply Cisco IOS IPS (inbound, outbound, or both)
- The location of the signature definition file (SDF)

For Cisco IOS 12.4(11) or later images, you are also prompted for the following information:

- Where you want to store files that contain changes to the IOS IPS configuration. A file that stores this type of information is referred to as a delta file.
- The public key to use to access the information in the delta files.
- The signature category. The basic signature category is appropriate for routers with less than 128 Mb of flash memory. The advanced signature category is appropriate for routers with more than 128 Mb of flash memory.

The use case scenario illustrates a configuration in which a Cisco IOS IPS rule is used. After you create the Cisco IOS IPS rule and deliver the configuration to the router, you can modify the rule by clicking the **Edit IPS** tab.

For more information on Cisco IOS IPS, see the documents at the following link:

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Click the **Launch IPS Rule Wizard** button to begin.

Create IPS: Welcome

This window provides a summary of the tasks to perform when you complete the IPS Rule wizard.

Click **Next** to begin configuring a Cisco IOS IPS rule.

Create IPS: Select Interfaces

Choose the interfaces on which you want to apply the Cisco IOS IPS rule by specifying whether the rule is to be applied to inbound traffic or outbound traffic. If you check both the inbound and the outbound boxes, the rule applies to traffic flowing in both directions.

For example: the following settings apply Cisco IOS IPS to inbound traffic on the BRI 0 interface, and both inbound and outbound traffic on the FastEthernet 0 interface.

Interface Name	Inbound	Outbound
BRI 0	Check	—
FastEthernet 0	Check	Check

Create IPS: SDF Location

Cisco IOS IPS examines traffic by comparing it against signatures contained in a signature definition file (SDF). The SDF can be located in router flash memory or on a remote system that the router can reach. You can specify multiple SDF locations so that if the router is not able to contact the first location, it can attempt to contact other locations until it obtains an SDF.

Use the **Add**, **Delete**, **Move Up**, and **Move Down** buttons to add, remove, and order a list of SDF locations that the router can attempt to contact to obtain an SDF. The router starts at the first entry, and works down the list until it obtains an SDF.

Cisco IOS images that support Cisco IOS IPS contain built-in signatures. If you check the box at the bottom of the window, the router will use the built-in signatures only if it cannot obtain an SDF from any location in the list.

Create IPS: Signature File

The Cisco IOS IPS signature file contains the default signature information present in each update to the file on Cisco.com. Any changes made to this configuration are saved in a delta file. For security, the delta file must be digitally signed. Specify the location of the signature file and provide the name and text of the public key that will be used to sign the delta file in this window.

This help topic describes the Signature File window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Specify the signature file you want to use with IOS IPS

If the signature file is already present on the PC, router flash memory, or on a remote system, click **Specify the signature file you want to use with IOS IPS** to display a dialog in which you can specify the signature file location.

Get the latest signature file from CCO and save to PC

Click **Get the latest signature file from CCO and save to PC** if the signature file is not yet present on the PC or in router flash memory. Click **Browse** to specify where you want to save the signature file, and then click **Download** to begin downloading the file. Cisco SDM downloads the signature file to the location that you specify.

Configure Public Key

Each change to the signature configuration is saved in the delta file. This file must be digitally signed with a public key. You can obtain a key from Cisco.com and paste the information in the Name and Key fields.

✎

Note   If you have already added a public key to the configuration using the Cisco IOS CLI, you must still provide a public key in this screen. After you have completed the Cisco IOS IPS Rule Wizard, you can go to **Edit IPS > Global Settings**. In the Global Settings screen, you can click **Edit** in the Edit IPS Prerequisites area, and then click **Public Key** to display the Public Key dialog. In that dialog, you can delete public keys that you do not need.

Follow these steps to place the public-key information in the Name and Key fields.

Step 1   Go to the following link to obtain the public key:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Step 2   Download the key to your PC.

Step 3   Copy the text after the phrase "named-key" into the Name field. For example, if the line of text including the name is the following:

```
named-key realm-cisco.pub signature
```

copy `realm-cisco.pub signature` to the Name field:

Step 4   Copy the text between the phrase `key-string`, and the word `quit` into the Key field. Example text follows:

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

Create IPS: Configuration File Location and Category

Specify a location for storing the signature information that the Cisco IOS IPS will use. This information consists of the signature file and the delta file that is created when changes are made to the signature information.

This help topic describes the Configuration File Location window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Config Location

Click the button to the right of the Config Location field to display a dialog that allows you to specify a location. After you enter information in that dialog, Cisco SDM displays the path to the location in this field.

Choose Category

Because router memory and resource constraints may prevent the use of all the available signatures, there are two categories of signatures—**basic** and **advanced**. In the Choose Category field, choose the category that will allow the Cisco IOS IPS to function efficiently on the router. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Add or Edit a Config Location

Specify a location for storing the signature information and the delta file that the Cisco IOS IPS will use.

Specify config location on this router

To specify a location on the router, click the button to the right of the Directory Name field and choose the directory in which you want to store the configuration information.

![pencil icon]

Note   If the router has a LEFS-based file system, you will be unable to create a directory in router memory. In this case, flash: is used as the config location.

Specify config location using URL

To specify a location on a remote system, specify the protocol and path of the URL needed to reach the location. For example, if you want to specify the URL http://172.27.108.5/ips-cfg, enter 172.27.108.5/ips-cfg.

![pencil icon]

Note   Do not include the protocol in the path that you enter. Cisco SDM adds the protocol automatically. If you enter the protocol, Cisco SDM displays an error message.

In the No. of Retries and Timeout fields, specify how many times the router is to attempt to contact the remote system, and how long the router is to wait for a response before stopping the contacting attempts.

Directory Selection

Click the folder in which you want to store configuration information. If you want to create a new folder, click **New Folder**, provide a name for it in the dialog displayed, select it, and click **OK**.

Signature File

Specify the location of the signature file that the Cisco IOS IPS will use.

Specify Signature File on Flash

If the signature file is located on router flash memory, click the button to the right of the field. Cisco SDM displays the signature file names of the correct format for you to choose.

Specify Signature File using URL

If the signature file is located on a remote system, select the protocol to be used, and enter the path to the file. For example, if the signature file IOS-S259-CLI.pkg is located at 10.10.10.5, and the FTP protocol will be used , select **ftp** as the protocol, and enter

```
10.10.10.5/IOS-S259-CLI.pkg
```

> **Note**   Do not include the protocol in the path that you enter. Cisco SDM adds the protocol automatically. If you enter the protocol, Cisco SDM displays an error message. Additionally, when you use an URL, you must specify a filename that conforms to the IOS-Snnn-CLI.pkg file naming convention, such as the file used in the previous example.

Specify Signature File on PC

If the signature file is located on the PC, click **Browse**, navigate to the folder containing the file, and select the filename. You must choose an Cisco SDM-specific package of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

Create IPS: Summary

Here is an example of a Cisco IOS IPS summary display on a router running a Cisco IOS release earlier than 121.4(11)T.

```
Selected Interface: FastEthernet 0/1

IPS Scanning Direction: Both

Signature Definition File Location: flash//sdmips.sdf

Built-in enabled: yes
```

In this example, Cisco IOS IPS is enabled on the FastEthernet 0/1 interface, and both inbound and outbound traffic is scanned. The SDF is named sdmips.sdf and is located in router flash memory. The router is configured to use the signature definitions built in to the Cisco IOS image that the router uses.

Create IPS: Summary

The Summary window displays the information that you have entered so that you can review it before delivering the changes to the router.

This help topic describes the Summary window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases. A sample Summary window display follows.

```
IPS rule will be applied to the outgoing traffic on the following interfaces.
     FastEthernet0/1
IPS rule will be applied to the incoming traffic on the following interfaces.
     FastEthernet0/0
Signature File location:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Public Key:
      30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Config Location
     flash:/configloc/
Selected category of signatures:
     advanced
```

In this example, the Cisco IOS IPS policy is applied to the FastEthernet 0/0 and the FastEthernet 0/1 interfaces. The signature file is located on the PC. The config location is on router flash memory, in a directory named configloc.

Edit IPS

In this window you can view the Cisco IOS IPS buttons for configuring and managing Cisco IOS IPS policies, security messages, signatures, and more.

IPS Policies Button

Click to display the Edit IPS window, where you can enable or disableCisco IOS IPS on an interface and view information about how Cisco IOS IPS is applied. If you enableCisco IOS IPS on an interface, you can optionally specify which traffic to examine for intrusion.

Global Settings Button

Click to display the Edit IPS: Global Settings window, where you make settings that affect the overall operation of Cisco IOS IPS.

Auto Update

This button appears if the Cisco IOS image on the router is version 12.4(11)T or later. Auto Update allows you to configure the router to obtain the latest signature updates from the Cisco Security Center automatically. Refer to Edit IPS: Auto Update for more information.

SEAP Configuration

This button appears if the Cisco IOS image on the router is version 12.4(11)T or later. Signature Event Action Processing (SEAP) gives you greater control over IOS IPS by providing advanced filtering and overrides.

SDEE Messages Button

Secure Device Event Exchange (SDEE) messages report on the progress of Cisco IOS IPS initialization and operation. Click to display the Edit IPS: SDEE Messages window, where you can review SDEE messages and filter them to display only error, status, or alert messages.

Signatures Button

Click to display the Edit IPS: Signatures window where you can manage signatures on the router.

NM CIDS Button

This button is visible if a Cisco Intrusion Detection System network module is installed in the router. Click to manage the IDS module.

Edit IPS: IPS Policies

This window displays the Cisco IOS IPS status of all router interfaces, and allows you to enable and disable Cisco IOS IPS on interfaces.

Interfaces

Use this list to filter the interfaces shown in the interface list area. Choose one of the following:

- All interfaces—All interfaces on the router.
- IPS interfaces—Interfaces on which Cisco IOS IPS has been enabled.

Enable Button

Click to enable Cisco IOS IPS on the specified interface. You can specify the traffic directions to which Cisco IOS IPS is to be applied, and the ACLs used to define the type of traffic you want to examine. See Enable or Edit IPS on an Interface for more information.

Edit Button

Click to edit the Cisco IOS IPS characteristics applied to the specified interface.

Disable Button

Click to disable Cisco IOS IPS on the specified interface. A context menu shows you the traffic directions on which Cisco IOS IPS has been applied, and you can choose the direction on which you want to disable Cisco IOS IPS. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco SDM dissociates any Cisco IOS IPS rules from that interface.

Disable All Button

Click to disable Cisco IOS IPS on all interfaces on which it has been enabled. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco SDM dissociates any Cisco IOS IPS rules from that interface.

Interface Name

The name of the interface. For example: Serial0/0, or FE0/1.

IP

This column can contain the following types of IP addresses:

- Configured IP address of the interface.

- DHCP client—The interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.

- Negotiated—The interface receives an IP address through negotiation with the remote device.

- Unnumbered—The router will use one of a pool of IP addresses supplied by your service provider for your router and for the devices on your LAN.

- Not applicable—The interface type cannot be assigned an IP address.

Inbound IPS/Outbound IPS

- Enabled—Cisco IOS IPS is enabled for this traffic direction.

- Disabled—Cisco IOS IPS is disabled for this traffic direction.

VFR Status

Virtual Fragment Reassembly (VFR) status. The possible values are:

- On—VFR is enabled.

- Off—VFR is disabled.

Cisco IOS IPS cannot identify the contents of IP fragments, nor can it gather port information from the fragment in order to match it with a signature. Therefore, fragments can pass through the network without being examined or without dynamic access control list (ACL) creation.

VFR enables the Cisco IOS Firewall to create the appropriate dynamic ACLs, thereby protecting the network from various fragmentation attacks.

Description

A description of the connection, if added.

IPS Filter Details

If no filter is applied to traffic, this area contains no entries. If a filter is applied, the name or number of the ACL is shown in parentheses.

Inbound and Outbound Filter Buttons

Click to view the entries of the filter applied to inbound or outbound traffic.

Field Descriptions

Action—Whether the traffic is permitted or denied.

✔️   Permit source traffic.

❌   Deny source traffic.

Source—Network or host address, or any host or network.

Destination—Network or host address, or any host or network.

Service—Type of service filtered: IP, TCP, UDP, IGMP, or ICMP.

Log—Whether or not denied traffic is logged.

Attributes—Options configured using the CLI.

Description—Any description provided.

Enable or Edit IPS on an Interface

Use this window to choose the interfaces on which you want to enable intrusion detection, and to specify the IPS filters for examining traffic.

Both, Inbound, and Outbound Buttons

Use these buttons to specify whether you are going to enable Cisco IOS IPS on both inbound and outbound traffic, only inbound traffic, or only outbound traffic.

Inbound Filter

(Optional) Enter the name or number of the access rule that specifies the inbound traffic to be examined. The ACL that you specify appears in the IPS Rules Configuration window when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

Outbound Filter

(Optional) Enter the name or number of the access rule that specifies the outbound traffic to be examined. The ACL that you specify appears in the IPS Rules Configuration window when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

... Button

Use this button to specify a filter. Click to display a menu with the following options:

- Choose an existing rule. See Select a Rule for more information.

- Create a new rule. See Add or Edit a Rule for more information.

- None (clear rule association). Use this option to remove a filter from a traffic direction to which it has been applied.

Enable fragment checking for this interface

(Enabled by default). Check if you want the Cisco IOS firewall to check for IP fragments on this interface. See VFR Status for more information.

Enable fragment checking on other interfaces

> If fragment checking is enabled for outbound traffic, the router must examine the inbound traffic that arrives on the interfaces that send outbound traffic to the interface being configured. Specify these interfaces below.

> If the Inbound radio button is chosen, this area does not appear.

Specify Signature File

> The Specify Signature File box contains information about the SDF version that the router is using, and enables you to update the SDF to a more recent version. To specify a new SDF, click the **...** button next to the Signature File field and specify a new file in the displayed dialog.

Edit IPS: Global Settings

> This window allows you to view and configure global settings for Cisco IPS. This help topic describes the information that you may see if the running Cisco IOS image is earlier than version 12.4(11)T.

Global Settings Table

> This table in the Global Settings window displays the current global settings and their values. Click **Edit** to change any of these values.

Item Name	Item Value
Syslog	If enabled, then notifications are sent to the syslog server specified in System Properties.
SDEE	Security Device Event Exchange. If enabled, SDEE events are generated.
SDEE Events	Number of SDEE events to store in the router buffer.
SDEE Subscription	Number of concurrent SDEE subscriptions.

Engine Options	The engine options are:
	• Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process.
	• Use Built-in Signatures (as backup)—If Cisco IOS IPS does not find signatures or fails to load them from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default.
	• Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.
Shun Events	This option uses the Shun Time parameter. Shun Time is the amount of time that shun actions are to be in effect. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Configured SDF Locations

A signature location is a URL that provides a path to an SDF. To find an SDF, the router attempts to contact the first location in the list. If it fails, it tries each subsequent location in turn until it finds an SDF.

Add Button

Click to add a URL to the list.

Edit Button

Click to edit a specified location.

Delete Button

Click to delete a specified location.

Move Up an d Move Down Buttons

Use to change the order of preference for the URLs in the list.

Reload Signatures

Click to recompile signatures in all signature engines. During the time that signatures are being recompiled in a signature engine, the Cisco IOS software can not use that engine's signatures to scan packets.

Edit Global Settings

Edit settings that affect the overall operation of Cisco IOS IPS in this window, in the Syslog and SDEE and Global Engine tabs.

Enable Syslog Notification (Syslog and SDEE Tab)

Check this checkbox to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE (Syslog and SDEE Tab)

Enter the number of concurrent SDEE subscriptions, in the range of 1–3, in the **Number of concurrent SDEE subscriptions** field. An SDEE subscription is a live feed of SDEE events.

In the **Maximum number of SDEE alerts to store** field, enter the maximum number of SDEE alerts that you want the router to store, in the range of 10–2000. Storing more alerts uses more router memory.

In the **Maximum number of SDEE messages to store** field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Enable Engine Fail Closed (Global Engine Tab)

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Use Built-in Signatures (as backup) (Global Engine Tab)

If Cisco IOS IPS does not find or fails to load signatures from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default.

Enable Deny Action on IPS interface (Global Engine Tab)

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Timeout (Global Engine Tab)

This option lets you set the number of minutes, in the range of 0–65535, that shun actions are to be in effect. The default value is 30 minutes. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Add or Edit a Signature Location

Specify the location from which Cisco IOS IPS should load an SDF. To specify multiple SDF locations, open this dialog again and enter the information for another SDF.

Specify SDF on this router

Specify the part of router memory in which the SDF is located by using the Location drop-down menu. For example: the menu could have the entries *disk0*, *usbflash1*, and *flash*. Then choose the filename by clicking the down arrow next to the File Name field or enter the filename in the File Name field.

Specify SDF using URL

If the SDF is located on a remote system, you can specify the URL at which it resides.

Protocol

Choose the protocol the router should use to obtain the SDF, such as *http* or *https*.

URL

Enter the URL in the following form:

path-to-signature-file

✎

Note The protocol you chose from the Protocol menu appears to the right of the URL field. Do *not* reenter the protocol in the URL field.

The following URL is provided as an example of the format. It is *not* a valid URL to a signature file, and it includes the protocol to show the full URL:

`https://172.16.122.204/mysigs/vsensor.sdf`

Autosave

Check this option if you want the router to automatically save the SDF if the router crashes. This eliminates the need for you to reconfigure Cisco IOS IPS with this SDF when the router comes back up.

Edit IPS: SDEE Messages

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to Cisco IOS IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All— SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

View By

> Choose the SDEE message field to search.

Criteria

> Enter the search string.

Go Button

> Click to initiate the search on the string entered in the Criteria field.

Type

> Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Time

> Time message was received.

Description

> Available description.

Refresh Button

> Click to check for new SDEE messages.

Close Button

> Click to close the SDEE Messages window.

SDEE Message Text

> This topic lists possible SDEE messages.

IDS Status Messages

Error Message

ENGINE_BUILDING: %s - %d signatures - %d of %d engines

> **Explanation** Triggered when Cisco IOS IPS begins building the signature microengine (SME).

Error Message

ENGINE_BUILD_SKIPPED: %s - there are no new signature definitions for this engine

> **Explanation** Triggered when there are no signature definitions or no changes to the existing signature definitions of an Intrusion Detection System SME.

Error Message

ENGINE_READY: %s - %d ms - packets for this engine will be scanned

> **Explanation** Triggered when an IDS SME is built and ready to scan packets.

Error Message

SDF_LOAD_SUCCESS: SDF loaded successfully from %s

> **Explanation** Triggered when an SDF file is loaded successfully from a given location.

Error Message

BUILTIN_SIGS: %s to load builtin signatures

> **Explanation** Triggered when the router resorts to loading the builtin signatures.

IDS Error Messages

Error Message

```
ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s
```

Explanation Triggered when Cisco IOS IPS fails to build one of the engines after an SDF file is loaded. One message is sent for each failed engine. This means that the Cisco IOS IPS engine failed to import signatures for the specified engine in the message. Insufficient memory is the most probable cause of this problem. If this happens, the new imported signature that belongs to this engine is discarded by Cisco IOS IPS.

Error Message

```
SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d
```

Explanation Triggered when an SDF file does not parse correctly.

Error Message

```
SDF_LOAD_FAILED: failed to %s SDF from %s
```

Explanation Triggered when an SDF file fails to load for some reason.

Error Message

```
DISABLED: %s - IDS disabled
```

Explanation   IDS has been disabled. The message should indicate the cause.

Error Message

```
SYSERROR: Unexpected error (%s) at line %d func %s() file %s
```

Explanation Triggered when an unexpected internal system error occurs.

Edit IPS: Global Settings

Several Cisco IOS IPS configuration options are available with Cisco IOS 12.4(11)T and later images. These are described in this help topic. Screen controls and configuration options available prior to Cisco IOS 12.4(11)T, such as the Syslog and SDEE global settings are described in Edit IPS: Global Settings.

This help topic describes the Global Settings window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Engine Options

The engine options available with Cisco IOS 12.4(11)T and later images are the following:

- Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process.

- Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.

Edit IPS Prerequisites Table

This table displays the information about how the router is provisioned for Cisco IOS IPS. Click **Edit** to change any of these values. The sample data in the following table indicated that the config location is the directory configloc in flash memory, that the router is using the basic category of signatures, and that a public key has been configured to allow the router to access the information in the configloc directory.

Item Name	Item Value
Config Location	flash:/configloc/
Selected Category	basic
Public Key	Configured

Edit Global Settings

The Edit Global Settings dialog contains a Syslog and SDEE tab, and a Global Engine tab. Click the link below for the information that you want to see:

- Syslog and SDEE Tab
- Global Engine Tab

Syslog and SDEE Tab

The Syslog and SDEE dialog displayed when the router uses a Cisco IOS 12.4(11)T or later image allows you to configure syslog notification and parameters for SDEE subscriptions, events and messages.

Enable Syslog Notification

Check this checkbox to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE

Enter the number of concurrent SDEE subscriptions, in the range of 1–3, in the Number of concurrent SDEE subscriptions field. An SDEE subscription is a live feed of SDEE events.

In the Maximum number of SDEE alerts to store field, enter the maximum number of SDEE alerts that you want the router to store, in the range of 10–2000. Storing more alerts uses more router memory.

In the Maximum number of SDEE messages to store field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Global Engine Tab

The Global Engine dialog displayed when the router uses a Cisco IOS 12.4(11)T or later image allows you to configure the settings described in the following sections.

Enable Engine Fail Closed

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Enable Deny Action on IPS interface

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Edit IPS Prerequisites

The Edit IPS Prerequisites dialog contains tabs for the following categories of information. Click on a link for the information that you want to see:

- Config Location Tab
- Category Selection Tab
- Public Key Tab

Config Location Tab

If a config location has been configured on the router, you can edit it. If none has been configured, you can click Add and configure one. The Add button is disabled if a config location is already configured. The Edit button is disabled when no config location has been configured. See Create IPS: Configuration File Location and Category for more information.

Category Selection Tab

If you specify a signature category, SDM configures the router with a subset of signatures appropriate for a specific amount of router memory. You can also remove an existing category configuration if you want to remove category constraints when selecting signatures.

Configure Category

Click **Configure Category** and choose either **basic** or **advanced**. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Delete Category

If you want to remove the category configuration, click **Delete Category**.

Public Key Tab

This dialog displays the public keys configured for Cisco IOS IPS. You can add keys or delete keys from this dialog. To add a key, click **Add** and configure the key in the dialog displayed.

To remove a key, select the key name and click **Delete**.

Add Public Key

You can copy the name of the key and the key itself from the following site on Cisco.com:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Copy the key name and paste it into the Name field in this dialog. Then copy the key from the same location and paste it into the Key field. For detailed instructions that explain exactly which parts of the text to copy and paste, see Configure Public Key.

Edit IPS: Auto Update

Signature file updates are posted on Cisco.com. Cisco SDM can download the signature file update that you specify, or it can automatically download the latest signature file update on a defined schedule.

This help topic describes the Auto Update window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Before Configuring Autoupdate

Before configuring autoupdate, you should synchronize the router clock with the clock on your PC. To do this, complete the following steps:

Step 1   Go to **Configure** > **Additional Tasks** > **Router Properties** > **Date/Time**.

Step 2   In the Date/Time window, click **Change Settings**.

Step 3   Check the **Synchronize with my local PC clock** option, and then click the **Synchronize** button.

Step 4   Close the dialog.

Download signature file from Cisco.com

To have Cisco SDM download a specific signature file from Cisco.com to your PC, specify the file that you want Cisco SDM to download, and specify the location where the file will be saved. Signature Package in use displays the version that the Cisco IOS IPS is currently using. A CCO login is required to download signature files and obtain other information from the Cisco.com the Cisco IOS IPS web pages.

To download the latest signature file, click **Get the latest file**. Click **Browse** to specify where you want the file saved, and then click **Download** to save the file to your PC.

To browse the available files before downloading, click **List the available files to download**. Then click the button to the right of the List of signature packages field. Click **Refresh** in the context menu to browse the list of available files. To view the readme file, click **Show readme**. Choose the file that you want, and then use the **Browse** and **Download** buttons to save it to your PC.

Autoupdate

Click **Enable Autoupdate** if you want Cisco SDM to automatically obtain updates from a remote server that you specify.

IPS Autoupdate URL Settings

Enter the username and password required to log in to the server, and enter the URL to the update file in the IPS Autoupdate URL Settings fields. A sample URL follows:

```
tftp//:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

Schedule

Specify a schedule for when you want the router to obtain the update from the server. You can specify multiple values in each column to indicate a range or to indicate multiple time values. To specify that you want to obtain the update from the server at 1:00 a.m. every day, Sunday through Thursday, choose the values in the following table.

Minute	Hour	Date	Day
0	1	Select 1 and select 31.	Check the boxes for Sunday through Thursday.

Click **Apply Changes** to send the changes that you make in the Auto Update fields to the router. Click **Discard Changes** to remove the data that you have entered in these fields.

Edit IPS: SEAP Configuration

Cisco IOS IPS available with Cisco IOS release 12.4(11)T or later implements Signature Event Action Processing (SEAP). This window describes SEAP features that you can configure. To begin configuration, click on one of the buttons under the SEAP Configuration button.

You can configure SEAP settings for Cisco IOS IPS when the router runs Cisco IOS 12.4(11)T and later releases.

Edit IPS: SEAP Configuration: Target Value Rating

The target value rating (TVR) is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

Use the buttons to the right of the Target Value Rating and Target IP Address columns to add, remove, and edit target entries. Click **Select All** to highlight all target value ratings automatically. Click **Add** to display a dialog in which you can create a new TVR entry. Click **Edit** to change the IP address information for an entry.

Target Value Rating Column

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. Once a target entry has been created, the rating cannot be changed. If you need to change the rating, you must delete the target entry and recreate it using the rating that you want.

Target IP Address Column

The target IP address can be a single IP address or a range of IP addresses. The following example shows two entries. One is a single IP address entry and the other is an address range.

Target Value Rating	Target IP Address
High	192.168.33.2
Medium	10.10.3.1-10.10.3.55

Apply Changes

When you have entered the information that you want in the Target Value Rating window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

To clear information that you have entered in the Target Value Rating window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes made that are awaiting delivery to the router.

Add Target Value Rating

To add a TVR entry, choose the target value rating and enter a Target IP Address or range of IP addresses.

Target Value Rating (TVR)

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. Once a rating has been used for one target entry, it cannot be used for additional entries. Therefore, enter into the same entry all the targets that you want to give the same rating.

Target IP Addresses

You can enter a single target IP address or a range of addresses, as shown in the examples that follow:

```
192.168.22.33
10.10.11.4-10.10.11.55
```

The IP addresses that you enter are displayed in the Target Value Rating window.

Edit IPS: SEAP Configuration: Event Action Overrides

Event action overrides allow you to change the actions associated with an event based on the Risk Rating RR of that event. You do this by assigning an RR range for each event action. If an event occurs and its RR falls within the range that you defined, the action is added to the event. Event action overrides are a way to add event actions globally without having to configure each signature individually.

Use Event Action Overrides

Check the Use Event Action Overrides box to enable Cisco IOS IPS to use event action overrides. You can add and edit event action overrides whether or not they are enabled on the router.

Select All

The Select All button works with the Enable, Disable and Delete buttons. If you want to enable or disable all event action overrides, click **Select All** and then click **Enable** or **Disable**. To remove all event action overrides, click **Select All**, and then click **Delete**.

Add and Edit Buttons

Click **Add** to display a dialog in which you can enter the information for an event action override. Choose an event action override, and click **Edit** to change the information for an event action override.

Delete

Click **Delete** to remove the event action overrides that you selected, or to remove all event action overrides if you clicked **Select All**.

Enable and Disable

The Enable and Disable buttons allow you to enable or disable event action overrides. Choose one event action override, or click **Select All** to enable or disable all event action overrides.

Apply Changes

When you have entered the information that you want in the Event Action Overrides window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

If you want to clear information that you have entered in the Event Action Overrides window but have not sent to the router, click **Discard Changes**. The **Discard Changes** button is disabled when there are no changes made that are awaiting delivery to the router.

Add or Edit an Event Action Override

To add an event action override, choose the event action, enable or disable it, and specify the RR range. If you are editing, you cannot change the event action.

Event Action

Choose one of the following event actions:

- Deny Attacker Inline—Does not transmit this packet and future packets from the attacker address for a specified period of time (inline only).

- Deny Connection Inline—Does not transmit this packet and future packets on the TCP Flow (inline only)

- Deny Packet Inline—Does not transmit this packet.

- Produce Alert—Writes an <evIdsAlert> to the log.

- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow.

Enabled

Click **Yes** to enable the event action override, or **No** to disable it. You can also enable and disable event action overrides in the Event Action Override window.

Risk Rating

Enter the lower bound of the RR range in the Min box, and the upper bound of the range in the Max box. When the RR value of an event falls within the range that you specify, Cisco IOS IPS adds the override specified by the Event Action. For example, if Deny Connection Inline is assigned a RR range of 90-100, and an event with an RR of 95 occurs, Cisco IOS IPS responds by denying the connection inline.

Edit IPS: SEAP Configuration: Event Action Filters

Event action filters let Cisco IOS IPS perform individual actions in response to an event without requiring it to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event. Event action filters are processed as an ordered list. You can move filters up or down in the list to have the router process one filter before it processes other filters.

The Event Action Filters window displays the configured event action filters, and allows you to reorder the filters list so that Cisco IOS IPS processes the filters in the order that you want.

Use Event Action Filters

Check **Use Event Action Filters** to enable the use of event action filters. You can add, edit, and remove event action filters, and rearrange the list to specify the order that the router processes the filters whether or not event action filtering is enabled.

Event Action Filter List Area

For a description of the columns in the Event Action Filter List area, see Add or Edit an Event Action Filter.

Event Action Filter List Buttons

The Event Action Filter List buttons allow you to create, edit, and remove event action filters, and to place each event action filter in the order you want it to be in the list. The buttons are described in the following sections.

Select All

The **Select All** button works with the **Enable**, **Disable**, and **Delete** buttons. To enable or disable all event action filters, click **Select All**, and then click **Enable** or **Disable**. To remove all event action filters, click **Select All**, and then click **Delete**.

Add

Click the **Add** button to add an event action filter to the end of the list. A dialog is displayed that enables you to enter the data for the filter.

Insert Before

To insert a new event action filter before an existing one, select the existing filter entry and click **Insert Before**. A dialog is displayed that enables you to enter the data for the filter.

Insert After

To insert a new event action filter after an existing one, select the existing filter entry and click **Insert Before**. A dialog is displayed that enables you to enter the data for the filter.

Move Up

Choose an event action filter and click the **Move Up** button to move the filter up in the list.

Move Down

Choose an event action filter and click the **Move Down** button to move the filter down in the list.

Edit

Click the **Edit** button to edit an event action filter you have chosen.

Enable

Click the **Enable** button to enable an event action filter you have chosen. To enable all event action filters, click **Select All** first, and then click **Enable**.

Disable

Click the **Disable** button to disable an event action filter you have chosen. To disable all event action filters, click **Select All** first, and then click **Disable**.

Delete

Click the **Delete** button to delete an event action filter you have chosen. If you want to delete all event action filters, click **Select All** first, and then click **Delete**.

Apply Changes

When you have entered the information that you want in this window, click **Apply Changes**. The Apply Changes button is disabled when there are no changes to send to the router.

Discard Changes

If you want to clear information that you have entered in this window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes awaiting delivery to the router.

Add or Edit an Event Action Filter

The following information describes the fields in the Add and the Edit Event Action Filter dialogs.

Name

SDM provides event action filter names beginning with Q00000, incrementing the numerical portion of the name by 1 each time you add an event action filter. You can also enter a name that you choose. If you are editing an event action filter, the Name field is read-only.

Enabled

Click **Yes** to enable the event action filter, or click **No** to disable it. You can also enable and disable event action filters in the Event Action Filter window.

Signature ID

For Signature ID, enter a range of signature IDs from 900 to 65535, or enter a single ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Subsignature ID

For Subsignature ID, enter a range of subsignature IDs from 0 to 255, or enter a single subsignature ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 70-200

Attacker Address

For Attacker Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Attacker Port

For Attacker Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Victim Address

For Victim Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, enter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key when you choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

> If you want the Cisco IOS IPS to stop when an event matches this event action
> filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against
> the other remaining filters, click **No**.

Comments

> You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

> Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of
> known attacks. Cisco IOS images that support Cisco IOS IPS have built-in
> signatures that can be used, and you can also have Cisco IOS IPS import
> signatures for the router to use when examining traffic. Imported signatures are
> stored in a signature definition file (SDF).
>
> This window lets you view the configured Cisco IOS IPS signatures on the router.
> You can add customized signatures, or import signatures from SDFs downloaded
> from Cisco.com. You can also edit, delete, enable, and disable signatures.
>
> Cisco IOS IPS is shipped with an SDF that contains signatures that your router
> can accommodate. To learn more about the SDF shipped with Cisco IOS IPS, and
> how to have Cisco IOS IPS use it, click IPS-Supplied Signature Definition Files.

Signature Tree

> The signature tree enables you to filter the signature list on the right according to
> the type of signature that you want to view. First choose the branch for the general
> type of signature that you want to display. The signature list displays the
> configured signatures for the type that you chose. If a plus (+) sign appears to the
> left of the branch, there are subcategories that you can use to refine the filter. Click
> the + sign to expand the branch and then choose the signature subcategory that
> you want to display. If the signature list is empty, there are no configured
> signatures available for that type.
>
> For example: If you want to display all attack signatures, click the **Attack** branch
> folder. If you want to see the subcategories that you can use to filter the display
> of attack signatures, click the + sign next to the Attack folder. If you want to see
> Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note   You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from Cisco. Click the following URL to download an SDF from Cisco.com (requires login):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*] New [*n*] Deleted [*n*]

This text gives you the count of new signatures and deleted signatures.

Select All

Click to choose all signatures in the list.

Add

Click **Add** if you want to do any of the following:

Cisco Router and Security Device Manager 2.5 User's Guide

- **Add New**—Choose this option to add a new signature, and provide signature parameters in the displayed dialog.

- **Clone**—The clone option is enabled if a signature is specified that does not belong to a hardcoded engine. It is disabled if the signature uses one of the the Cisco IOS hardcoded engines.

Edit

Click to edit the parameters of the specified signature.

Delete

Click **Delete** to mark the specified signature for deletion from the list. To view signatures you have deleted, click **Details**. For more information on the status and handling of these signatures, see Signatures marked for deletion.

> **Note**   You can display and monitor TrendMicro OPACL signatures, but you cannot edit, delete, enable, or disable them. If a TrendMicro OPACL signature is specified, the **Edit**, **Delete**, **Enable** and **Disable** buttons are disabled. The Cisco Incident Control Server assumes control of these signatures.

Enable

Click **Enable** to enable the specified signature. An enabled signature is designated with a green checkmark. A signature that was disabled and then enabled has a yellow Wait icon in the ! column indicating that the change must be applied to the router.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Summary or Details Button

Click to display or hide the signatures marked for deletion.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

![Note icon] **Note**   Signatures that are set to import and are identical to deployed signatures will not be imported and will not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out.
	Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.
	![yellow wait icon]
	This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example: the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example: ICMP Echo Reply.
Action	Action to take when the signature is detected.
Filter	ACL associated with the corresponding signature.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco SDM displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.

- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.

- Restore Defaults—Click to restore the signature's default values.

- Remove Filter—Click to remove a filter applied to the signature.

- NSDB help (need CCO account)—Click to display help on the Network Security Data Base (NSDB).

Signatures marked for deletion

This area is visible when the **Details** button is clicked. It lists the signatures that you deleted from the Signature List, and signatures that are marked for deletion because imported signatures are set to replace signatures already configured on the router. See How to Import Signatures for more information.

Signatures marked for deletion remain active in the Cisco IOS IPS configuration until you click **Apply Changes**. If you exit the Signatures window and disable Cisco IOS IPS, the marked signatures will be deleted if Cisco IOS IPS is re-enabled.

Undelete All Button

Click to restore all signatures in the signatures marked deleted list.

Undelete Button

Click to restore specified signatures marked for deletion. When clicked the signatures are unmarked, and returned to the list of active signatures.

Apply Changes Button

Click to deliver newly imported signatures, signature edits, and newly enabled or disabled signatures to the router. When the changes are applied, the yellow Wait icon is removed from the ! column. These changes are saved to your router flash memory in the file sdmips.sdf. This file is created automatically the first time you click **Apply Changes**.

> **Note** If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Apply Changes** button is disabled.

Discard Changes Button

Click to discard accumulated changes.

> **Note** If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Discard Changes** button is disabled.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, nter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key when you choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

If you want the Cisco IOS IPS to stop when an event matches this event action filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against the other remaining filters, click **No**.

Comments

You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that Cisco IOS IPS can use, and you can also have Cisco IOS IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This help topic describes the Signatures window displayed when the router runs Cisco IOS 12.4(11)T and later releases.

The Signatures window lets you view the configured Cisco IOS IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, enable, disable, retire, and unretire signatures.

Signature Tree

The signature tree enables you to filter the signature list on the right according to the type of signature that you want to view. First choose the branch for the general type of signature that you want to display. The signature list displays the configured signatures for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click the + sign to expand the branch and then choose the signature subcategory that you want to display. If the signature list is empty, there are no configured signatures available for that type.

For example: If you want to display all attack signatures, click the **Attack** branch folder. If you want to see the subcategories that you can use to filter the display of attack signatures, click the + sign next to the Attack folder. If you want to see Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from Cisco. Click the following URL to download an SDF from Cisco.com (requires login):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*]

This text gives you the total number of signatures on the router.

Select All

Click to choose all signatures in the list.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*]

This text gives you the total number of signatures on the router.

Select All

Click to choose all signatures in the list.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Retire

Click **Retire** to prevent a signature from being compiled for scanning.

Unretire

Click **Unretire** to allow the signature to be compiled for scanning.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

Note Signatures that are set to import and are identical to deployed signatures will not be imported and will not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out.
	Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.
	This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example: the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example: ICMP Echo Reply.
Action	Action to take when the signature is detected.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high
Fidelity Rating	The fidelity rating of the signature.
Retired	A value of true or false. True if signature has been retired. False if not. Retired signatures are not compiled.
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco SDM displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.

- Fidelity Rating—Click to enter a fidelity rating for the signature.

- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.

- Restore Defaults—Click to restore the signature's default values.

• NSDB help (need CCO account)—Click to display help on the Network
Security Data Base (NSDB).

Apply Changes

Click **Apply Changes** to deliver newly imported signatures, signature edits, and
newly enabled or disabled signatures to the router. When the changes are applied,
the yellow Wait icon is removed from the ! column. These changes are saved to
your router flash memory in the file sdmips.sdf. This file is created automatically
the first time you click **Apply Changes**.

> **Note**   If you are attempting to import signatures, and these signatures are all identical to
> deployed signatures, then the **Apply Changes** button is disabled.

Discard Changes

Click **Discard Changes** to discard accumulated changes.

> **Note**   If you are attempting to import signatures, and these signatures are all identical to
> deployed signatures, then the **Discard Changes** button is disabled.

Edit Signature

Use the fields in Edit Signature dialog to edit the selected signature. The changes
that you make are stored in a delta file that is saved to router flash memory. The
elements of signatures are described in the following sections.

This help topic describes the Edit Signatures window displayed when the router
runs Cisco IOS 12.4(11)T and later releases.

Signature ID

The unique numerical value assigned to this signature. This value allows the Cisco
IOS IPS to identify a particular signature.

Subsignature ID

The unique numerical value assigned to this subsignature. A subsignature ID is used to identify a more granular version of a broad signature.

Alert Severity

Choose one of the following to categorize the severity of the alert: High, Medium, Low, or Informational.

Sig Fidelity Rating

The signature fidelity rating is a value set by the author of the signature to quantify the confidence that the signature will produce true positives. This value is set before a signature is deployed and can be adjusted when signature performance data is available.

Promiscuous Delta

The promiscuous delta is a factor that is subtracted from the risk rating (RR) of an event when the router is operating in promiscuous mode. The Promiscuous Delta is subtracted from the RR every time an alert is triggered when the system is deployed in promiscuous mode.

Note   Even though the promiscuous delta can be reconfigured on a signature basis, it is not recommended that you change any of the predefined promiscuous-delta settings.

Sig Description

The signature description includes the signature name and release, any alert notes available from the Cisco Security Center, user comments, and other information.

Engine

The signature engine associated with this signature. One commonly-used engine is named Atomic IP.

The Engine box contains fields that allow you to tune a wide variety of signature parameters. For example, you can specify the action to be taken if this signature is matched and an event is generated, you can specify the layer 4 protocol to inspect for events matching this signature, and you can specify IP parameters, such as header length and type of service.

Event Counter

The controls in the Event Counter box allow you to specify the parameters described in the following sections.

Event Count

The number of times an event must occur before an alert is generated.

Event Count Key

The type of information to use to count an event as occurring. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, the count increments by 1. If you choose **attacker address**, only that piece of information is needed.

Event Interval

The number of seconds between events being sent to the log. If you select **Yes**, an additional field is displayed allowing you to enter the number of seconds.

Alert Frequency

The purpose of the alert frequency parameter is to reduce the volume of the alerts written to the log,

Summary Mode

There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing.

Summary Key

The type of information to use to determine when to summarize. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, summarization occursY. If you choose **attacker address**, only that piece of information is needed.

Specify Global Summary Threshold

You can optionally specify numerical thresholds to use for determining when to summarize events to the log. If you choose **Yes**, you can specify a global summary threshold, and a summary interval.

Status

You can specify whether the signature should be enabled, disabled, or retired in the Status box. Additionally, the Status box can display the signatures that you have obsoleted.

File Selection

This window allows you to load a file from your router. Only DOSFS file systems can be viewed in this window.

The left side of window displays an expandable tree representing the directory system on your Cisco router flash memory and on USB devices connected to that router.

The right side of the window displays a list of the names of the files and directories found in the directory that is specified in the left side of the window. It also shows the size of each file in bytes, and the date and time each file and directory was last modified.

You can choose a file to load in the list on the right side of the window. Below the list of files is a Filename field containing the full path of the specified file.

Note   If you are choosing a configuration file to provision your router, the file must be a CCCD file or have a .cfg extension.

Name

Click **Name** to order the files and directories alphabetically based on name. Clicking **Name** again will reverse the order.

Size

Click **Size** to order the files and directories by size. Directories always have a size of zero bytes, even if they are not empty. Clicking **Size** again will reverse the order.

Time Modified

Click **Time Modified** to order the files and directories based on modification date and time. Clicking **Time Modified** again will reverse the order.

Assign Actions

This window contains the actions that can be taken upon a signature match. Available actions depend on the signature, but the most common actions are listed below:

- **alarm**—Generate an alarm message. Same as **produce-verbose-alert**.

- **deny-attacker-inline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **denyAttackerInline**.

- **deny-connection-inline**—Drop the packet and all future packets on this TCP flow. Same as **produce-alert** and **denyFlowInline**.

- **deny-packet-inline**—Do not transmit this packet (inline only). Same as **drop**.

- **denyAttackerInline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **deny-attacker-inline**.

- **denyFlowInline**—Create an ACL that denies all traffic from the IP address that is considered the source of the attack belonging to the 5-tuple (src ip, src port, dst ip, dst port and l4 protocol). denyFlowInline is more granular than denyAttackerInline. Same as **produce-alert** and **deny-connection-inline**.

- **drop**—Drop the offending packet. Same as **deny-packet-inline**.

- **produce-alert**—Generate an alert. Same as **denyFlowInline** and **deny-connection-inline**.

- **produce-verbose-alert**—Generate an alert which includes an encoded dump of the offending packet. Same as **alarm**.

- **reset**—Reset the connection and drop the offending packet. Same as **reset-tcp-connection**.

- **reset-tcp-connection**—Send TCP RESETS to terminate the TCP flow. Same as **reset**.

Import Signatures

Use the Import IPS window to import signatures from an SDF or other file on your PC. The information in this window tells you which signatures are available from the SDF, and which of them are already deployed on your router.

How to Import Signatures

To import signatures, follow these steps:

Step 1   Use the signature tree, View By drop-down list, and Criteria List drop-down list to display the signatures you want to import.

In the signature list, uncheck the **Import** checkbox for the signatures that you *do not* want to import. If you want to uncheck the **Import** checkbox for all of the signatures, click the **Unselect All** button, which changes to the **Select All** button

Step 2   Check the checkbox **Do not import signatures that are defined as disabled** if you want to avoid importing signatures that may degrade router performance when used.

Step 3   Click the **Merge** button to merge the imported signatures with the signatures that are already configured on the router, or the **Replace** button to replace the already configured signatures.

See Merge Button and Replace Button for more information.

Step 4   Click the **Apply Changes** button in the Edit IPS window to deploy the imported signatures.

You can make changes to the imported signatures before deploying them. Signatures that set to import and are identical to deployed signatures will not be imported. If all imported signatures are identical to deployed signatures, then the **Apply Changes** button is disabled.

Signature Tree

If you need a description of the signature tree, click this link: Signature Tree. You can use the signature tree in this window to assemble the signatures that you want to import, category by category.

For example: you may want to add signatures from the OS category, and from the Service category. You can do this by choosing the **OS** branch of the tree, and any branch from that part of the tree that you want, such as the UNIX branch or the Windows branch. When the types of signatures that you want to import are displayed, you can make your selections in the signature list area. Then you can choose the **Service** branch, and choose any of the service signatures that you want.

View By and Criteria List

The View By and Criteria list boxes enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By list, then choose the value for that criteria in the list to the right (the criteria list).

For example: If you choose **Engine** in the View By list, the criteria list is labeled Engine, and you can choose among the available engines, such as **Atomic.ICMP**, and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria list.

Signature List Area

The signature list displays the signatures available in the SDF based on the criteria you chose in the signature tree. The text of signatures already found on the target router is blue.

The signature list area has these columns:

- Sig ID—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- Name—Name of the signature. For example: *FTP Improper Address*.

- Severity—High, medium, low, or informational.

- Deployed—Displays *Yes* if the signature is already deployed on the router. Displays *No* if the signature is not deployed on the router.

- Import—Contains a checkbox for each signature. If you want to import the signature, check this box.

Note All of the signatures imported from an SDF or a zip file with the name IOS-S*xxx*.zip can be displayed in the signature list. When signatures are imported from a zip file with a different name, only the signatures found through the View By and Criteria List drop-down lists are displayed.

Merge Button

Click to merge the signatures that you are importing with the signatures that are already configured on the router.

Replace Button

Click to replace the signatures that are already configured on the router with the signatures that you are importing. Signatures already configured on the router but that are *not* found in the list of signatures being imported are marked for deletion and listed under **Signatures Marked for Deletion** in **Edit IPS > Signatures**. See Signatures marked for deletion for more information.

Add, Edit, or Clone Signature

This window contains fields and values described in the Field Definitions section. The fields vary depending on the signature, so this is not an exhaustive list of all the fields you might see.

Field Definitions

The following fields are in the Add, Edit, and Clone Signature windows.

- **SIGID**—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- **SigName**—Name assigned to the signature.

- **SubSig**—Unique numerical value assigned to this subsignature. A subsig ID is used to identify a more granular version of a broad signature.

- **AlarmInterval**—Special Handling for timed events. Use AlarmInterval Y with MinHits X for X alarms in Y second interval.

- **AlarmSeverity**—Severity of the alarm for this signature.

- **AlarmThrottle**—Technique used for triggering alarms.

- **AlarmTraits**—User-defined traits further describing this signature.

- **ChokeThreshold**—Threshold value of alarms-per-interval that triggers autoswitch AlarmThrottle modes. If ChokeThreshold is defined, Cisco IOS IPS automatically switches AlarmThrottle modes if a large volume of alarms is seen in the ThrottleInterval.

- **Enabled**—Identifies whether or not the signature is enabled. A signature must be enabled in order for Cisco IOS IPS to protect against the traffic specified by the signature.

- **EventAction**—Actions Cisco IOS IPS will take if this signature is triggered.

- **FlipAddr**—True if the source and destination addresses, and their associated ports, are swapped in the alarm message. False if no swap occurs (default).

- **MinHits**—Specifies the minimum number of signature hits that must occur before the alarm message is sent. A hit is the appearance of the signature on the address key.

- **SigComment**—Comment or description text for the signature.

- **SigVersion**—Signature version.

- **ThrottleInterval**—Number of seconds defining an Alarm Throttle interval. This is used with the AlarmThrottle parameter to tune special alarm limiters.

- **WantFrag**—True enables inspection of fragmented packets only. False enables inspection of non-fragmented packets only. Choose "undefined" to allow for inspection of both fragmented and non-fragmented packets.

Cisco Security Center

The Cisco Security Center provides information on emerging threats, and links to the Cisco IOS IPS signatures available to protect your network from them. Signature reports and downloads are available at this link (requires login):

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

IPS-Supplied Signature Definition Files

To ensure that the router has as many signatures available as its memory can accommodate, Cisco SDM is shipped with one of the following SDFs:

- 256MB.sdf—If the amount of RAM available is greater than 256 MB. The 256MB.sdf file contains 500 signatures.

- 128MB.sdf—If the amount of RAM available is between 128 MB and 256 MB. The 128MB.sdf file contains 300 signatures.

- attack-drop.sdf—If the amount of available RAM is 127 MB or less. The attack-drop.sdf file contains 82 signatures.

If your router runs Cisco IOS version 12.4(11)T or later, you must use an SDF file that has a name of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

> **Note**   The router must be running Cisco IOS Release 12.3(14)T or later releases to be able to use all the available signature engines in 256MB.sdf and 128MB.sdf files. If the router uses an earlier release, not all signature engines will be available.

To use an SDF in router memory, determine which SDF has been installed and then configure Cisco IOS IPS to use it. The procedures that follow show you how to do this.

Determine Which SDF File Is in Memory

To determine which SDF file is in router memory, open a Telnet session to the router, and enter the **show flash** command. The output will be similar to the following:

```
System flash directory:
```

```
File   Length   Name/status
  1    10895320  c1710-k9o3sy-mz.123-8.T.bin
  2    1187840  ips.tar
  3    252103   attack-drop.sdf
  4    1038     home.shtml
  5    1814     sdmconfig-1710.cfg
  6    113152   home.tar
  7    758272   es.tar
  8    818176   common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

In this example, the attack-drop.sdf file is in router memory. On some routers, such as routers with a disk file system, use the **dir** command to display the contents of router memory.

Configuring IPS to Use an SDF

To haveCisco IOS IPS use the SDF in router memory, do the following:

Step 1   Click **Global Settings**.

Step 2   In the Configured SDF Locations list, click **Add**.

Step 3   In the dialog box displayed, click **Specify SDF on flash**, and enter the name of the SDF file.

Step 4   Click **OK** to close the dialog box.

Security Dashboard

The Security Dashboard allows you to keep your router updated with signatures for the latest security threats. You must have Cisco IOS IPS configured on your router before you can deploy signatures using the Security Dashboard.

Top Threats Table

The Top Threats table displays the latest top threats from Cisco if the status of the associated signatures indicates that they are available for deployment or are under investigation. Some of the top threats in the table are associated with signatures that can be deployed to your router. The text of signatures already found on your router is blue.

To obtain the latest top threats, click the **Update top threats list** button.

Note   You cannot update the top threats by using the Cisco SDM **Refresh** button or your browser's Refresh command.

The top threats table has the following columns:

- **Device Status** indicates if the signature associated with the threat is already enabled on your router. The following symbol may appear in the Device Status column:

    Signature is already enabled on your router.

    Signature is not available on your router or is available but *not* enabled on your router.

- **Sig ID** is a unique number identifying the signature associated with the threat.
- **SubSig ID** is a unique number identifying the subsignature. If the signature associated with the threat does not have a subsignature, **SubSig ID** is 0.
- **Name** is the name given to the threat.
- **Urgency** indicates if the level of the threat is high (Priority Maintenance) or normal (Standard Maintenance).
- **Threat Status** indicates if the signature associated with the threat is available or if the threat is still under investigation.
- **Deploy** contains checkboxes that can be checked if the signature associated with the threat is available to deploy.

Select SDF

Click the **Browse** button and choose the Cisco IOS SDF file to use. The Cisco IOS SDF file must be present on your PC. The format that the filename has depends on the version of Cisco IOS the router is running.

- If the router is running a Cisco IOS image earlier than 12.4(11)T, the SDF must have a name with the format IOS-S*xxx*.zip, where *xxx* is a three-digit number. For example: a Cisco IOS IPS SDF file may be named IOS-S193.zip.

- If the router is running a Cisco IOS image of version 12.4(11)T or later, the SDF must have a name with the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip

The location of a Cisco IOS SDF file you choose is shown in the SDF file location field. The SDF file location field is read-only.

After the first time you download a Cisco IOS SDF file, Cisco SDM remembers the location of the file. The next time you load the Security Dashboard, Cisco SDM will select the latest Cisco IOS SDF file based on the three-digit number in the file's name.

Note The Cisco IOS SDF file with the highest three-digit number in its name is the latest Cisco IOS SDF file.

Deploying Signatures From the Top Threats Table

Before attempting to deploy signatures from the Top Threats table, ensure that you have:

- Configured Cisco IOS IPS on your router
- Downloaded the latest Cisco IOS file to your PC

To deploy signatures from the Top Threats table, follow these steps:

Step 1 Click the **Update top threats list** button to ensure that you have the latest top threats list.

Step 2 In the Deploy column, check the checkbox for each top-threat signature you want to deploy from the Top Threats table.

Only top threats with the status **Signature available** can be chosen. Available signatures with a red icon in their Applied column are automatically set to deploy.

Step 3   Click the **Browse** button and choose the latest Cisco IOS file if you need to ensure that you are using the latest signature file.

You may need to do this if the location of the latest SDF file has changed since it was last set in the Security Dashboard, or if the format of its name is not IOS-S*xxx*.zip, where *xxx* is a three-digit number

Step 4   Click the **Deploy signatures** button to deploy the chosen signatures to your router.

A warning is shown if any of the chosen signatures are not found in the Cisco IOS file. However, all found signatures can still be deployed. After being deployed on your router, the signatures are automatically enabled and added to the router active signatures list.

IPS Migration

If you have an existing the Cisco IOS IPS configuration that you want to migrate to Cisco IOS IPS available in Cisco IOS 12.4(11)T or later releases, you can use the IPS Migration wizard to do the migration.

Note   If the router uses a Cisco IOS image of version 12.4(11)T or later, you must migrate a configuration created before this release if you want to use Cisco IOS IPS on your router. If you do not migrate the configuration, the configuration commands will not be changed, but Cisco IOS IPS will not operate.

Click the **Launch IPS Migration Wizard** button to begin the migration process.

Migration Wizard: Welcome

The Migration Wizard Welcome window lists the tasks that the wizard helps you to complete. If you do not want to run the IPS migration wizard, click **Cancel**.

The IPS Migration wizard is available when the router runs Cisco IOS 12.4(11)T and later releases.

Migration Wizard: Choose the IOS IPS Backup Signature File

The backup file contains the Cisco IOS IPS information that will be migrated. This may be a Signature Definition File (SDF), such as attack-drop.sdf, or 128MB.sdf. If you made changes to the signature information, such as disabling signatures or changing the attributes of specific signatures, the records of your changes are kept in a separate file. If you used Cisco SDM to make changes, Cisco SDM saves them in a file named sdmips.sdf, which it saves to router flash memory. If you made changes manually, you may have given the file another name and may have saved a backup copy on your PC.

Click the **...** button next to the backup file field to display a dialog that allows you to browse for this backup file on router flash memory or on your PC.

Signature File

Specify the location of the backup signature file in this dialog.

Specify signature file on flash

If the backup signature file is located on flash memory, click the down arrowhead button next to this field and choose the file.

Specify signature file on the PC

If the backup signature file is located on the PC, click the **Browse** button next to this field and navigate to the file.

Java Heap Size

Cisco SDM displays the Java Heap Size window when the Java heap size is too low to support an SDM feature. Complete the following procedure to set the heap size to the value stated in the window.

Step 1   Exit Cisco SDM.

Step 2   Click **Start > Control Panel > Java**.

Step 3   Open the Java Runtime Settings dialog. The location of this dialog varies by release.

    a.   Click the **Advanced** tab. Locate the Java Runtime Settings dialog and proceed to Step 4. If the dialog is not available from the Advanced tab, proceed to b.

    b.   Click the **Java** tab. Locate the Java Runtime Settings dialog. Click the **View** button if necessary to display the dialog, and proceed to Step 4.

Step 4   In the Java Runtime Parameters column, enter the value stated in the window. For example if the window states that you must use the value -Xmx256m, enter that value in the Java Runtime Parameters column. The following table shows sample values.

Product Name	Version	Location	Java Runtime Parameters
JRE	1.5.0_08	C:\Program Files\java\jre1.5.0_08	-Xmx256m

Step 5   Click **OK** in the Java Runtime Settings dialog.

Step 6   Click **Apply** in the Java Control Panel, and then click **OK**.

Step 7   Restart Cisco SDM.

Java Heap Size

Network Module Management

If the router has network modules that are managed by other applications, such as Intrusion Detection System (IDS), Secure Router Device Manager (Cisco SDM) provides a means for you to launch those applications.

IDS Network Module Management

If a Cisco IDS Network Module is installed on the router, this window displays basic status information for it. If the IDS Network Module has been configured, you will also be able to start the Intrusion Detection Device Manager (IDM) software on the IDS Network Module, and select the router interfaces that you want the IDS Network Module to monitor from this window.

If Cisco SDM detects that the IDS Network Module has not been configured, it prompts you to open a session to the network module so that you can configure it. You can use Telnet or SSH for this session.

IDS Network Module Control Buttons

Cisco SDM enables you to issue a number of basic commands to the IDS Network Module from this window.

Reload

Click to reload the IDS network module operating system.

Reset

Click to perform a reset of the IDS network module hardware You should only use the Reset button to recover from Failed state, or after you have shutdown the IDS Network Module.

Shutdown

Click to shutdown the IDS Network Module. You should always perform a shutdown before you to remove the module from the router.

Launch IDM

Click to start the IDM software on the IDS module. When you launch the IDM software, Cisco SDM displays a dialog box that asks you for the IP address of the IDS module's external Fast Ethernet interface. When Cisco SDM obtains the correct address, it opens an IDM window. For more information on this dialog box, refer to IP Address Determination.

For more information on how to run the IDM application, refer to the documents at the following link:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Refresh

Click to refresh the status display.

IDS Network Module Status

This area shows the general status of the IDS Network Module. It contains the following types of information.

- Service Module–The name of the network module.

- State–The state of the network module. Possible states are: Steady state, Shutdown, and/or Failed.

- Software Version–The version of IDM software running on the module.

- Model–The model number of the network module.

- Memory–The amount of memory available on the network module.

IDS NM Monitoring Interface Settings

This area of the window shows which router interfaces have traffic sent to the IDS network module for monitoring.

✔	A check mark icon next to the interface name indicates that the IDS network module is monitoring the traffic on that interface.
✖	A red icon with an X next to the interface name indicates that the IDS network module is not monitoring the traffic on that interface.

Configure

Click to add or remove interfaces from this list. When you click **Configure**, Cisco SDM verifies that the IDS Network Module has been configured, and that the router has all the configuration settings necessary to communicate with the IDS Network Module. If any configurations are not in place, Cisco SDM displays a checklist showing you what has been configured and what has not been configured. You can click on the items that have not been configured to complete the configuration, and then have Cisco SDM reverify that these items have been configured so that you can then add or remove interfaces from the IDS Network Module Interface Settings list.

IDS Sensor Interface IP Address

Cisco SDM must communicate with the IDS network module using the IP address of the module's internal Fast Ethernet interface. This window appears when Cisco SDM cannot detect this IP address, and enables you to supply one without leaving Cisco SDM to do so. If the IDS network module has been configured with a static IP address, or configured as IP unnumbered to another interface with an IP address, this window will not appear.

Entering an IP address in this window may create a new loopback interface. Loopback interfaces can be displayed in the Interfaces and Connections window. The IP address you enter will only be seen by the router. Therefore, it can be any address you want to use.

IP Address

Enter an IP address to use for the IDS Sensor interface. Cisco SDM will do the following:

- Create a loopback interface. The number 255 is used if available, if not, another number will be used. This loopback interface will be listed in the Interfaces and Connections window.

- Configure the loopback interface with the IP address you enter.

- Configure the IDS network module IP unnumbered to the loopback interface.

- If the IDS network module has already been configured IP unnumbered to an existing loopback interface, but the interface does not have a valid IP address, the loopback interface is given the IP address you enter in this window.

IP Address Determination

Cisco SDM displays this window when it needs to determine the IP address of a network module that you are attempting to manage. This is typically the IP address of the module's external Ethernet interface. Cisco SDM can use the address it used the last time the management application was run, it can attempt to discover the IP address, or it can accept an address that you provide in this window.

Select a method, and click **OK**. If the method you choose fails, you can select another method.

Use Cisco SDM last known IP Address

Click to have Cisco SDM use the IP address that it used the last time that the management application for this network module was run. If the IP address of module has not been changed since the management application was last run, and you do not want Cisco SDM to attempt discovery of the address, use this option.

Let Cisco SDM discover IP address

Click to have Cisco SDM attempt to discover the network module's IP address. You can use this option if you do not know the IP address, and you are not sure that the last address Cisco SDM used to contact the network module is still correct.

Specify

> If you know the network module's IP address, choose this option, and enter the address. Cisco SDM will remember the address, and you can select **Use SDM last known IP Address** the next time you start the network module.

IDS NM Configuration Checklist

> This window is displayed when you have clicked **Configure** in the IDS Network Module Management window to specify the router interfaces whose traffic is to be analyzed, but the IDS network module or the router lacks a configuration setting required for the two devices to communicate. It shows which configuration settings are needed, and in some cases, allows you to complete the configuration from within Cisco SDM.

> ✔ A check mark icon in the Action column means the configuration setting has been made.

> ✖ An X icon in the Action column means that the configuration setting must be made in order for the router to be able to communicate with the IDS network module.

IDS NM Sensor Interface

> ✖ If this row contains an X icon in the Action column, the IDS NM Sensor interface has not been configured with an IP address. Double-click the row and enter an IP address for the IDS Sensor in the dialog displayed. The IDS Sensor IP address is the address that Cisco SDM and the router use when communicating with the IDS network module. This IP address can be a private address; no hosts other than the router it is installed in will be able to reach the address.

Date & Time

✖   If this row contains an X icon in the Action column, the router's clock settings have not been configured. Double-click on this row, and enter time and date settings in the Date and Time Properties window.

IP CEF Setting

✖   If this row contains an X icon in the Action column, Cisco Express Forwarding (CEF) has not been enabled on the router. Double-click on this row, and click **Yes** to enable IP CEF on the router.

IDS NM Initial Setup

✖   If this row contains an X icon in the Action column, Cisco SDM has detected that the IDS Network Module's default IP address has not been changed. Double-click on this row, and Cisco SDM will prompt you to open a session to the IDS module and complete configuration. You can use Telnet or SSH for this session.

For more information on configuring the IDS module, refer to the documents at the following link.

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Refresh

✖   After you have fixed configuration settings, you can click this button to refresh the checklist. If an X icon remains in the Action column, a configuration setting has still not been made.

IDS NM Interface Monitoring Configuration

Use this window to select router interfaces whose traffic you want the IDS network module to monitor.

Monitored Interfaces

This lists contains the interfaces whose traffic the IDS network module is monitoring. To add an interface to this list, select an interface from the Available Interfaces list, and click the left arrow (**<<**) button. To remove an interface from this list select the interface and click the right arrow (**>>**) button.

Available Interfaces

This lists contains the interfaces whose traffic the IDS network module is not currently monitoring. To add an interface to the Monitoring Interfaces list, select the interface, and click the left arrow (**<<**) button.

Network Module Login

Enter the username and password required to login to the network module. These credentials may not be the same credentials required to log in to the router.

Feature Unavailable

This window appears when you try to configure a feature that the Cisco IOS image on your router does not support. If you want to use this feature, obtain a Cisco IOS image from Cisco.com that supports it.

Switch Module Interface Selection

This window is displayed when there is more than one switch module installed on the router, and allows you to select the one that you want to manage. Click the radio button next to the switch module that you want to manage, and then click **OK**.

Quality of Service

The Quality of Service (QoS) Wizard allows a network administrator to enable Quality of Service (QoS) on the router's WAN interfaces. QoS can also be enabled on IPSec VPN interfaces and tunnels. The QoS edit windows enables the administrator to edit policies created using the wizard.

Creating a QoS Policy

Complete these steps to create a QoS policy:

Step 1   If you want to review the Cisco IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **QoS**.

Step 4   In the Create QoS Policy tab, click **Launch QoS Wizard**.

Step 5   Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 6   Cisco SDM displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7   To send the configuration to the router, click **Finish**.

Step 8   If you checked **Preview commands before delivering to router** in the Edit
Preferences screen, the Cisco IOS CLI commands that you are sending are
displayed. Click **Deliver** to send the configuration to the router, or click **Cancel**
to discard it. If you did not make this setting, clicking Finish sends the
configuration to the router.

Create a QoS Policy Reference describes the configuration screens.

Create a QoS Policy Reference

The topics in this section describe the configuration screens.

- Create QoS Policy
- QoS Wizard
- Interface Selection
- Queuing for Outbound Traffic
- Add a New Traffic Class
- Policing for Outbound Traffic
- QoS Policy Generation
- QoS Configuration Summary

Create QoS Policy

The QoS Wizard allows a network administrator to enable Quality of Service
(QoS) on the router's WAN interfaces. QoS can also be enabled on IPSec VPN
interfaces and tunnels.

The policy is applied to outgoing traffic on the interface.

To create a QoS policy, click **Launch QoS Wizard**.

QoS Wizard

This window summarizes the information that you will be providing as you complete the QoS Policy wizard.

Click the **Next** button to begin configuring a QoS policy.

Interface Selection

Choose the interface on which you want to configure the QoS policy in this window. This window lists WAN interfaces, and interfaces which do not have a configured outbound QoS policy. VPN interfaces are included in the list, but interfaces used for Easy VPN clients, and interfaces with an existing QoS policy are not included.

If the router Cisco IOS image release is 12.4(11)T or later, virtual template tunnel interfaces may appear in this list. If you choose a VTI interface, you will be able to configure shaping and queuing parameters.

Field Reference

Table 29-1   Interface Selection

Element	Description
Details	To view configuration details about the chosen interface, click **Details**. The window displays the interface's IP address and subnet mask, names of access rules and policies applied to the interface, and connections the interface is used for.

Table 29-1   Interface Selection (continued)

Element	Description
DSCP marking (trusted)	To use Differentiated Services Code Point (DSCP) markings to classify traffic, click **DSCP marking (trusted)**. Cisco network devices such as IP phones and switches add DSCP markings to packets. Configuring DSCP on the router allows these markings to be used to classify traffic. If the Cisco IOS image on the router does not support DSCP marking, this option will not appear.
NBAR protocol discovery (untrusted)	To use Networked Based Application Recognition (NBAR) protocol discovery to classify traffic, click **NBAR protocol discovery (untrusted)**. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by classifying packets and then applying Quality of Service (QoS) to the classified traffic. If the Cisco IOS image on the router does not support NBAR protocol discovery, this option will not appear.

Queuing for Outbound Traffic

In this screen, configure queuing for outbound traffic.

Field Reference

Table 29-2 describes the fields in this screen.

Table 29-2   Queuing for Outbound Traffic

Element	Description
Configure Shaping	
To configure shaping for outbound traffic, click **Configure Shaping**.	
Committed Information Rate	The Committed Information Rate (CIR) is the rate at which the interface is to transfer data. Enter the CIR in kilobits per second.
Bandwidth Allocation	
Traffic Class	A traffic class is a specific type of traffic, such as voice traffic and routing traffic. The Cisco SDM default traffic classes and user-created traffic classes are listed in this column.

Table 29-2   Queuing for Outbound Traffic (continued)

Element	Description
Bandwidth Percentage	To specify the bandwidth percentage for a traffic class, enter the percentage value for that class. Traffic types that depend on high transmission rates, such as voice traffic, should be given a higher percentage than traffic classes that do not need high transmission rates, such as routing traffic. The Cisco SDM default traffic classes are displayed with suggested values. When you change the percentage value of any traffic class, the best effort class adjusts to a higher or lower value. The total bandwidth of all classes other than best effort cannot exceed 75%.
Allocated Bandwidth	Cisco SDM displays the Allotted Bandwidth column when you configure a QoS policy for a non-VTI interface. It displays the kilobits per second allotted to the traffic class based on the CIR and the bandwidth percentage entered.
Add Class	To add a traffic class to this policy, click **Add Class** and enter the class information in the displayed dialog.
Remove	To remove a traffic class from this list that you have created, select the list and click **Remove**. Cisco SDM default classes cannot be removed.

Add a New Traffic Class

Add a new traffic class in this screen.

Field Reference

Table 29-3 describes the fields in this screen.

Table 29-3   Add New Traffic Class Fields

Element	Description
Class Name	Enter a name for the traffic class.

Table 29-3 *Add New Traffic Class Fields (continued)*

Element	Description
Classification	
Match	Specify whether the QoS class is to look for matches to Any or to All of the selected criteria. If you choose **Any**, traffic must meet only one of the match criteria. If you choose **All**, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column.
	Any—Click **Any** to specify that traffic must meet only one of the criteria specified in the classification list that you create.
	All—Click **All** to specify that traffic must meet all the criteria specified in the classification list that you create.
Item Name	This column displays the types of criteria that you can include in this traffic class. If the QoS policy uses NBAR protocol discovery, you can specify protocol and ACL values. If the QoS policy uses DSCP marking, you can specify DSCP values as well as protocol and ACL values.
Item Value	This column displays the values configured for the particular type, separated by commas. For example, the Protocol row might show the following values: `http, edonkey, dhcp`
Edit	To add or edit the values for a particular type of entry, select the type, and click **Edit**. Then, add or modify entries for type in the displayed dialog.
Bandwidth Percentage	Enter the bandwidth percentage that you want to give to the class. Cisco SDM displays a message if you enter a value that causes the total percentage value of all traffic types other than best effort to exceed 75%. If that occurs, lower the percentage value.
Use LLQ (Low Latency Queuing)	To have LLQ be used for this traffic class, click **Use LLQ** (**Low Latency Queuing**).

Policing for Outbound Traffic

Configure policing for outbound traffic in this screen.

Field Reference

Table 29-4 describes the fields in this screen.

Table 29-4   *Policing for Outbound Traffic Fields*

Element	Description
Configure policing for outbound traffic	If you want the QoS policy to include policing for outbound traffic, check this option and enter values in the configuration fields. Otherwise, click **Next** to proceed to the next screen.

Policing causes packets that exceed the Committed Information Rate (CIR) to be dropped. |
| Traffic Class | This column lists the traffic classes included in this QoS policy. |
| Committed Information Rate (CIR) | Enter the CIR for each traffic class. The bandwidth of the link is listed at the bottom of the screen. Cisco SDM displays a message if any entered value causes the total to exceed the link bandwidth. |

QoS Policy Generation

Use this window to allocate the bandwidth to the different types of traffic carried on the selected interface. The percentage value that you enter represents 1000 Kbps. For example, if you enter 5%, a bandwidth of 5000 Kbps is allocated. The total percentage value for all types of traffic excluding Best Effort cannot exceed 75%.

Field Reference

Table 29-5   *QoS Policy Generation*

Element	Description
Voice	Voice traffic. The default value is 33 percent of the bandwidth.
Call Signalling	Signalling needed to control voice traffic. The default value is 5 percent of the bandwidth
Routing	Traffic generated by this and other routers to manage the routing of packets. The default value is 5 percent of the bandwidth.
Management	Telnet, SSH and other traffic generated to manage the router. The default value is 5 percent of the bandwidth.
Transactional	Examples would be traffic generated for retail applications, or database updates. The default value is 5 percent of the bandwidth.
Best Effort	Remaining bandwidth for other traffic, such as e-mail traffic. The default value is 47 percent of the bandwidth. The value of Best Effort is dynamically updated based on the total percentage for the other types of traffic.

QoS Configuration Summary

The QoS Wizard Summary window displays a summary of the QoS policy created based on your choices in the wizard. This policy map will be attached to the selected interface. Each class that the SDM QoS wizard configures is summarized in this screen. A partial display follows. showing the interface that the policy is bound to, the classification type (NBAR or DSCP), the policy name, and several of the QoS classes created.

```
Interface:  FastEthernet0/0

Classification:  DSCP

Policy Name: SDM-QoS-Policy-1

Policy Details


-----------------------------------------------------------------------
Class Name: SDM-Voice-1
-----------------------------------------------------------------------
Enabled: Yes
```

```
Match DSCP: ef
Queuing: LLQ
Bandwidth Percentage: 33


------------------------------------------------------------------------
Class Name: SDM-Signalling-1
------------------------------------------------------------------------
Enabled: Yes
Match DSCP: cs3,af31
Queuing: CBWFQ
Bandwidth Percentage: 5


------------------------------------------------------------------------
Class Name: SDM-Routing-1
------------------------------------------------------------------------
Enabled: Yes
Match DSCP: cs6
Queuing: CBWFQ
Bandwidth Percentage: 5


------------------------------------------------------------------------
Class Name: class-default
------------------------------------------------------------------------
Enabled: Yes
Match Protocols:
Queuing: Fair Queue
Random Detect: Yes


------------------------------------------------------------------------
Class Name: SDM-Streaming-Video-1
------------------------------------------------------------------------
Enabled: No
Match DSCP: cs4
```

Editing QoS Policies

Complete these steps to edit a QoS policy:

Step 1   If you want to review the Cisco IOS CLI commands that you send to the router
when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit
> Preferences > Preview commands before delivering to router**. The preview
screen allows you to cancel the configuration if you want to.

Step 2 In the Cisco SDM toolbar, click **Configure**.

Step 3 In the Cisco SDM taskbar, click **QoS**.

Step 4 Click **Edit QoS Policy**.

Step 5 Choose the QoS policy that you want to edit.

Step 6 Click **Edit**. Then, make changes to the settings in the displayed dialogs.

Step 7 Click OK to close the dialog and send the changes to the router.

Step 8 If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it. If you did not make this setting, clicking Finish sends the configuration to the router.

Edit QoS Policy Reference describes the configuration screens.

Edit QoS Policy Reference

The topics in this section describe the configuration screens.

- Edit QoS Policy
- Associate or Disassociate the QoS Policy
- Add or Edit a QoS Class
- Edit Match DSCP Values
- Edit Match Protocol Values
- Add Custom Protocols
- Edit Match ACL

Edit QoS Policy

The **Edit QoS Policy** window allows you to view and change configured QoS policies, and associate policies with router interfaces. This help topic contains separate sections for different parts of the screen. To view the information for a section, click on the section heading.

Policy Selection Reference

Table 29-6   *Policy Selection Area*

Element	Description
View Policy on interface	Choose the interface whose QoS policies you want to view.
In Direction	Choose the traffic direction on which the policy that you want to view is applied.
Go	To view the policy for the interface and traffic direction that you chose, click **Go**.
Associate	To change the association of a QoS policy with an interface, click **Associate**. If the policy is currently associated with an interface, you can disassociate the policy, or change the traffic direction the policy is applied to. The Associate button is disabled when a frame-relay serial interface is displayed in the View Policy on Interface field.
Policy Name	This field displays the name of the policy associated with the interface and traffic direction that you chose.

QoS Class Button Reference

Table 29-7   *QoS Buttons*

Element	Description
Add	To add a QoS class to the policy, click **Add**.
Edit	To edit a QoS class in this screen, choose the class and click **Edit**. The Edit button is disabled when a read-only Qos class is selected.
Delete	To remove a QoS class from this policy, select a class and click **Delete**. The Delete button is disabled when a read-only Qos class is selected.
Cut	To remove a class from its current position in the list, select the class and click **Cut**. Use the Paste button to place the class in the position that you want. The Cut button is disabled when a read-only Qos class is selected.
Copy	To copy class information, select the class and click **Copy**. The Copy button is disabled when a read-only Qos class is selected.

Table 29-7   QoS Buttons (continued)

Element	Description
Paste	To edit copied class information and provide a new name for the class, click **Paste**. If you choose **Add this class to the policy**, the class will be placed with the enabled polices in the class. The Paste button is disabled when a read-only Qos class is selected.
Move Up	To move a class up the class list, choose a class and click **Move Up**. This button can only be used to move enabled classes. The Move Up button is disabled when a read-only Qos class is selected.
Move Down	To move a class down the class list, choose a class and click **Move Down**. This button can only be used to move enabled classes. The Move Down button is disabled when a read-only Qos class is selected.
Add Service Policy	To add a service policy to an existing QoS policy, select an existing class name from the policy, click **Add Service Policy**, and choose whether to add a new service policy or use an existing policy.
Remove Service Policy	To remove a service policy, choose the top-level class-default entry, and click **Remove Service Policy**.
Apply Changes	Changes that you make in this window are not immediately delivered to the router. To deliver changes that you make, click **Apply Changes**.
Discard Changes	If you do not want the changes that you have made in this window to be sent to the router, click **Discard Changes**.

Class List Display Reference

Table 29-8   Class List Display Area

Element	Description
	If this icon appears next to the QoS class, it is read-only, and it cannot be edited, deleted, or moved to another position in the class list.
Class Name	The name of the QoS class. Cisco SDM predefines names for QoS classes.

Table 29-8   Class List Display Area (continued)

Element	Description
Match	Whether the QoS class looks for matches to **Any** or to **All** of the selected DSCP values. If you choose **Any**, traffic must meet only one of the match criteria. If you choose **All**, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column.
Classification	This portion of the display contains the following columns: • DSCP—The DSCP values that are chosen for possible match. • Protocols—The protocols included in this QoS class. A video traffic QoS class might have protocols such as cuseeme, netshow, and vdolive. A routing traffic QoS class might have protocols such as BGP, EIGRP, and OSPF. • ACL—The name or number of an ACL that specifies the traffic that this QoS class applies to.
Action	This portion of the display contains the following columns: • Queuing—This column lists the queuing type, Class Based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ), or Fair Queuing, and displays the bandwidth allocated to the class. • Shaping—This column displays Yes if shaping is configured for this policy, or No if shaping is not configured. • Policing—This column displays Yes if policing is configured for this policy, or No if policing is not configured. • Set DSCP—The DSCP value that is given to this type of traffic by the QoS class. • Drop—The column displays Yes if this type of traffic is to be dropped, or No if it is not to be dropped.

Add Class for the New Policy

Add a traffic class for a new QoS policy in this screen.

Field Reference

Table 29-9 describes the fields in this screen.

Table 29-9   Add Class for New Policy

Element	Description
Policy Name	Enter a name for the QoS Policy.
Class Name	Enter a name for the traffic class.
Classification	
Match	Specify whether the QoS class is to look for matches to Any or to All of the selected criteria. If you choose **Any**, traffic must meet only one of the match criteria. If you choose **All**, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column. • Any—Click **Any** to specify that traffic must meet only one of the criteria specified in the classification list that you create. • All—Click **All** to specify that traffic must meet all the criteria specified in the classification list that you create.
Item Name	This column displays the types of criteria that you can include in this traffic class. If the QoS policy uses NBAR protocol discovery, you can specify protocol and ACL values. If the QoS policy uses DSCP marking, you can specify DSCP values as well as protocol and ACL values.
Item Value	This column displays the values configured for the particular type, separated by commas. For example, the Protocol row might show the following values: `http, edonkey, dhcp`
Edit	To add or edit the values for a particular type of entry, select the type, and click **Edit**. Then, add or modify entries for type in the displayed dialog.

Add Service Policy to Class

In this screen, add an existing service policy to a QoS class.

Table 29-10   Add Service Policy to Class

Element	Description
Existing service policy	Select an existing service policy from the list.

Associate or Disassociate the QoS Policy

Use this window to change the associations that a QoS policy has to router interfaces and traffic directions.

Field Reference

Table 29-11

Element	Description
Interface	This column lists the router interfaces. To choose an interface to which you want to associate the QoS policy, check the box next to the interface name.
	Note If you select the interface Cisco SDM uses to communicate with the router, you cause the connection between SDM and the router to be dropped.
Inbound	To associate the QoS policy to inbound traffic on the chosen interface, check the box in this column.
Outbound	To associate the QoS policy to outbound traffic on the chosen interface, check the box in this column.

Add or Edit a QoS Class

You can create and edit QoS traffic classes, and specify whether the class is to be added to the QoS policy.

Field Reference

Table 29-12   Add or Edit a QoS Class

Element	Description
Add this class to the policy	To include this QoS class in QoS policy, check **Add this class to the policy**. If this option is not checked, then the selected QoS class is marked as Disabled in the Edit QoS Policy window.
Class Name	The QoS class name is displayed in this field if you are editing an existing class. You must enter a classname if you are adding a new class to a policy, or pasting information from a QoS class that you have copied.
Class Default	This option appears when there is no class-default in the QoS policy. To add class-default—the default class—instead of creating a new class, click **Class Default**. There are several configuration parameters that you cannot set for class-default: • Classification box—You cannot specify classification criteria. • Action box—You cannot specify that traffic be dropped. Additionally, you can only specify that Fair Queuing be used.

Table 29-12   Add or Edit a QoS Class (continued)

Element	Description
Classification	Choose the types of items and values that you want the router to examine traffic for. If you click All, traffic must match all criteria. If you click Any, traffic need only match a single criterion. You must specify a value type in the list and click **Edit** to specify the values. To specify that the class is to match http, edonkey, and smtp, for example, choose **Protocol**, and click **Edit**. Then choose those protocols in the Edit Match Protocol Values dialog and click **OK**. The protocols that you chose appear in the Value column of the Classification list.
	If you want the class to match traffic defined in an ACL, click **Access Rule**, and then click **Edit**. In the dialog that appears, you can choose an existing ACL, create a new one, or clear existing associations if you are editing a QoS class.

Table 29-12   Add or Edit a QoS Class (continued)

Element	Description
Action	Choose the action that the router is to take when it finds traffic that matches the specified DSCP values.
	• **Drop**—Drop the traffic. If you select **Drop**, other options in the Action area are disabled.
	• **Set DSCP**— Choose the DSCP value that you want the traffic to be reset to.
	• **Queuing**— LLQ is available if the traffic uses the RTP protocol or has a DSCP value of EF. If the traffic does not have these attributes, the LLQ option is not available. If you are adding or editing the default class—class-default—only Fair Queuing is available.
	• **Bandwidth Percentage**—The percentage value that you enter is used as an absolute percentage of the total bandwidth on the interface.
	• **Bandwidth Remaining Percentage**—The percentage value that you enter is used as a relative percentage of the total bandwidth on the interface. For instance, you can specify that 30 percent of the available bandwidth be allocated to one class, and 60 percent of the bandwidth be allocated to another QoS class. To use this option, all other classes must use this option. The **Bandwidth Remaining Percentage** option is disabled if **LLQ** is selected.
	• **Random Detect**—Enables Weighted Random Early Detection (WRED) and Distributed WRED (DWRED) on the router. This option is disabled if **LLQ** is selected. Random Early Detection drops packets during periods of high congestion, thus telling the source host to decrease the transmission rate.

Edit Match DSCP Values

To add a DSCP value to the match list, choose a value from the **Available DSCP Values** column on the left, and click the top double-arrowhead button to add it to the **Selected DSCP Values** column. To remove a value from the **Selected DSCP Values** column, choose the value and click the bottom double-arrowhead button.

Edit Match Protocol Values

To add a protocol to a class, choose a protocol from the Available Protocol Values column on the left, and click the top double-arrowhead button to add it to the Selected Protocol Values column. To remove a protocol from the Selected Protocol Values column, choose the protocol and click the bottom double-arrowhead button.

Add Custom Protocols

This window allows you to add custom protocols that are not available in the Edit Match Protocol Values window. Do the following to define a custom protocol:

Step 1   Select the name of the custom protocol from the Name list.

Step 2   Select whether it will be used as a TCP or a UDP protocol.

Step 3   Define the port numbers that this protocol will use. Enter a port number in the New Port Number field, and click **Add** to add it to the Port Numbers list. To remove a port number from the list, choose the number and click **Remove**.

Edit Match ACL

Choose either **Select an existing rule (ACL)**, or **Create a new rule (ACL) and select**. Additional dialogs are displayed to enable you to create or select an existing rule. If you want to clear existing rule associations, you can choose **None (clear associations)**.

Configure Policing

In this screen, configure policing for a QoS policy.

Field Reference

Table 29-13 describes the fields in this screen.

Table 29-13   *Configure Policing*

Element	Description
Specify the access rate parameters for policing	
Committed Information Rate (CIR)	Enter the CIR to be used for the policy in kilobits per second. When the traffic rate reaches the CIR, excess traffic is dropped or remarked.
Normal Burst Size (BC)	Optional. Enter the normal burst size in kilobits per second. The normal burst size determines how large traffic bursts can be before some traffic exceeds the CIR.
Excess Burst Size (BE)	Optional. Enter the excess burst size in kilobits per second. The excess burst size determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.
Action Type	This column lists the names of the actions that you can choose for traffic that conforms to, exceeds, or violates the configured CIR, BC, and BE parameters.
Action	Choose what you want the router to do when traffic conditions conform, exceed or violate configured policing parameters. The conform and the exceed actions are mandatory and have default values. The violate action is optional. The available actions are the following: • Drop—(Default for exceed action) Discard the packet. • None—(Available for violate action) • Set DSCP Transmit—Set the DSCP and transmit. • Transmit—(Default for conform action) Send the packet.
Optional parameters	Optional parameters are enabled when you choose the Set DSCP Transmit action. The options displayed are the available DSCP markings.

Configure Shaping

In this screen, configure shaping for a QoS policy.

Field Reference

Table 29-14 describes the fields in this screen.

Table 29-14   Configure Shaping

Element	Description
Committed Information Rate (CIR)	Enter the CIR to be used for the policy in kilobits per second. When the traffic rate reaches the CIR, excess traffic is dropped or remarked.
Normal Burst Size (BC)	Optional. Enter the normal burst size in kilobits per second. The normal burst size determines how large traffic bursts can be before some traffic exceeds the CIR.
Excess Burst Size (BE)	Optional. Enter the excess burst size in kilobits per second. The excess burst size determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.

Configure Queuing

In this screen, configure queuing for a QoS policy. The fields displayed change based on the queuing method chosen. You can choose the following queuing methods:

- LLQ— Low Latency Queuing
- CBWFQ—Class-Based Weighted Fair Queuing
- Fair Queue—Weighted Fair Queuing (WFQ)

Field Reference

Table 29-15 describes the fields in this screen.

Table 29-15   Configure Queuing Fields

Element	Description
LLQ Chosen	
Priority Percentage	Bandwidth is allocated as an absolute percentage of the total bandwidth of the interface or tunnel. Enter a percentage value from 1 to 100 to specify the amount of bandwidth that you want to use.
CBWFQ Chosen	
Bandwidth	Bandwidth is allocated as an absolute percentage of the total bandwidth of the interface or tunnel. Enter a percentage value from 1 to 100 to specify the amount of bandwidth that you want to use.
Bandwidth Remaining	Bandwidth is allocated as a relative percentage of the total bandwidth available on the interface. Enter a percentage value from 1 to 100 to specify the amount of available bandwidth that you want to use.
Random Detect	To enable Weighted Random Early Detection (WRED), click **Random Detect**.
Fair Queue Chosen	
Queue Limit	Enter the number of packets to allow in the queue.
Random Detect	To enable Weighted Random Early Detection (WRED), click **Random Detect**.

Network Admission Control

Network Admission Control (NAC) protects data networks from computer viruses by assessing the health of client workstations, ensuring that they receive the latest available virus signature updates, and controlling their access to the network.

NAC works with antivirus software to assess the condition of a client, called the client's *posture*, before allowing the client access to the network. NAC ensures that a network client has an up-to-date virus signature set which has not been infected. If the client requires a signature update, NAC directs it to complete the update. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment until disinfection is completed.

For more information on NAC, click the following links:

- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Create NAC Tab

You use the Create NAC tab and NAC wizard to create a NAC policy and associate it with an interface. After you create the NAC policy, you can edit it by clicking **Edit NAC** and choosing it in the policy list.

The NAC configuration on the router is only one part of a complete NAC implementation. Click Other Tasks in a NAC Implementation to learn the tasks that must be performed on other devices in order to implement NAC.

Enable AAA Button

Authentication, authorization, and accounting (AAA) must be enabled on the router before you can configure NAC. If AAA is not enabled, click the **Enable AAA** button. If AAA has already been configured on the router, this button is not displayed.

Launch NAC Wizard Button

Click this button to launch the NAC wizard. The wizard divides NAC configuration into a series of screens in which you complete a single configuration task.

How Do I List

If you want to create a configuration that this wizard does not guide you through, click the button next to this list. It lists other types of configurations that you might want to perform. If you want to learn how to create one of the configurations listed, choose the configuration and click **Go**.

Other Tasks in a NAC Implementation

A full NAC implementation includes the following configuration steps:

Step 1   Install and configure the Cisco Trust Agent (CTA) software on network hosts. This provides hosts with a posture agent capable of responding to EAPoUDP queries by the router. See the links after these steps to obtain the CTA software and learn how to install and configure it.

Step 2   Install and configure an AAA authentication EAPoUDP server. This server must be a Cisco Secure Access Control Server (ACS) using the RADIUS protocol. Cisco Secure Access Control Server software version 3.3 is required. See the links after these steps to learn more about installing and configuring ACS.

Step 3   Install and configure the posture validation and remediation server.

If you are a registered Cisco.com user, you can download Cisco Trust Agent (CTA) software from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

The document at the following link explains how to install and configure CTA software on a host.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

The document at the following link contains an overview of the configuration process.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Documents at the following link explain how to install and configure Cisco Secure ACS for Windows Servers version 3.3.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

Welcome

The NAC wizard enables you to do the following:

- Choose the interface on which NAC is to be enabled—Hosts attempting access to the network through this interface must undergo the NAC validation process.

- Configure NAC Policy Servers—Admission control polices are configured on these servers, and the router contacts them when a network host attempts to access the network. You can specify information for multiple servers. NAC policy servers use the RADIUS protocol.

- Configure a NAC exception list—Hosts such as printers, IP phones, and hosts without NAC posture agents installed may need to bypass the NAC process. Hosts with static IP addresses and other devices can be identified in an exception list, and be handled using an associated exception policy. Hosts can also be identified by their MAC address, or by their device type.

- Configure an agentless host policy—If you want to use a policy residing on a Cisco Secure ACS server to handle hosts without an installed posture agent, you can do so. When the Cisco Secure ACS server receives a packet from an agentless host, it responds by sending the agentless host policy. Configuring an agentless host policy is useful when there are agentless hosts that are dynamically addressed, such as DHCP clients.

- Configuring NAC for remote access—Hosts using Cisco SDM to manage the router must be allowed access. The wizard lets you specify IP addresses for remote management so that Cisco SDM can modify the NAC ACL to allow the hosts with those addresses access to the router.

Configuring NAC on the router is the last step in a NAC configuration. Before you configure the router with this feature, Complete the steps described in the following link: Other Tasks in a NAC Implementation.

NAC Policy Servers

NAC admission control policies are configured and stored in a policy database residing on RADIUS servers running Cisco Secure ACS version 3.3. The router must validate the credentials of network hosts by communicating with the RADIUS server. Use this window to provide the information the router needs to contact the RADIUS servers. Each RADIUS server that you specify must have Cisco Secure Cisco Access Control Server (ACS) software version 3.3 installed and configured.

Choose the RADIUS client source

Configuring the RADIUS source allows you to specify the source IP address to be sent in RADIUS packets bound for the RADIUS server. If you need more information about an interface, choose the interface and click the **Details** button.

The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco ACS version 3.3 or later.

If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of the interface through which the RADIUS packets exit the router.

If you choose an interface, the source IP address in the RADIUS packets will be the address of the interface that you chose as the RADIUS client source.

> **Note**   Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.

Details Button

If you need a quick snapshot of the information about an interface before choosing it, click **Details**. The screen shows you the IP address and subnet mask, the access rules and inspection rules applied to the interface, the IPSec policy and QoS policy applied, and whether there is an Easy VPN configuration on the interface.

Server IP, Timeout, and Parameters Columns

The Server IP, Timeout, and Parameters columns contain the information that the router uses to contact a RADIUS server. If no RADIUS server information is associated with the chosen interface, these columns are blank.

Use for NAC Check Box

Check this box if you want to use the listed RADIUS server for NAC. The server must have the required admissions control policies configured if NAC is to be able to use the server.

Add, Edit, and Ping Buttons

To provide information for a RADIUS server, click the **Add** button and enter the information in the screen displayed. Choose a row and click **Edit** to modify the information for a RADIUS server. Choose a row and click **Ping** to test the connection between the router and a RADIUS server.

> **Note** When performing a ping test, enter the IP address of the RADIUS source interface in the source field in the ping dialog. If you chose **Router chooses source**, you need not provide any value in the ping dialog source field.

The **Edit** and **Ping** buttons are disabled when no RADIUS server information is available for the chosen interface.

Interface Selection

Choose the interface on which to enable NAC in this window. Choose the interface through which network hosts connect to the network.

Click the **Details** button to display the policies and rules associated with the interface you choose. The window displays the names of the ACLs applied to inbound and to outbound traffic on this interface.

If an inbound ACL is already present on the interface, Cisco SDM uses that ACL for NAC by adding appropriate permit statements for EAPoUDP traffic. If the IP address of the interface on which NAC is being applied were 192.55.22.33, a sample permit statement might be the following:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

The permit statement that Cisco SDM adds uses the port number 21862 for the EAPoUDP protocol. If the network hosts run EAPoUDP on a custom port number, you must modify this ACL entry to use the port number that the hosts use.

If no inbound ACL is configured on the interface you specify, you can have Cisco SDM apply an ACL to the interface. You can choose a recommended policy, or a policy that simply monitors reported NAC postures.

- **Strict Validation (Recommended)**—Cisco SDM applies an ACL that denies all traffic (**deny ip any any**). Admission to the network is determined by the NAC validation process. By default, all traffic is denied except the traffic found to be valid based on the policy configured on the NAC policy server.

- **Monitor NAC Postures**—Cisco SDM applies an ACL that permits all traffic (**permit ip any any**). After the NAC validation process, the router may receive policies from the NAC server that deny access to certain hosts. You can use the **Monitor NAC Postures** setting to determine the impact of NAC configuration on the network. After you have done so, you can modify the

policies on the NAC policy server, and then reconfigure NAC on the router to use **Strict Validation**, by changing the ACL applied to the interface to **deny ip any any** using the Cisco SDM Firewall Policy feature.

NAC Exception List

You can identify hosts that must be allowed to bypass the NAC validation process. Typically, hosts such as printers, IP phones, and hosts without NAC posture agent software installed are added to the exception list.

If there are hosts without static addresses on your network it is recommended that they be entered in the agentless host policy, and not in the NAC exception list. The NAC exception policy may not work properly if host IP addresses change.

If you are using the NAC wizard and you do not need to configure a NAC exception list, you can click **Next** without entering information in this window. As an alternative or as a complement to the NAC exception list, the wizard allows you to configure an agentless host policy in another window.

IP Address/MAC Address/Device Type, Address/Device, and Policy Columns

These columns contain information about a host in the exception list. A host can be identified by its IP address, MAC address, or the type of device it is. If it is identified by an address, the IP address or MAC address is shown in the row along with the name of the policy that governs the host access to the network.

Add, Edit, and Delete Buttons

Build the exception list by clicking **Add** and entering information about a host. You can use the **Add** button as many times as you need to.

Choose a row and click **Edit** to change information about a host. Click **Delete** to remove information about a host from this window. The Edit and Delete buttons are disabled when there is no information in this list.

Add or Edit an Exception List Entry

Add or edit the information in an exception list entry in this window.

Type List

Hosts are chosen by the way they are identified. This list contains the following selections:

- IP Address—Choose this if you want to identify the host by its IP address.

- MAC Address—Choose this if you want to identify the host by its MAC address.

- Cisco IP Phone—Choose this if you want to include the Cisco IP phones on the network in the exception list.

Specify Address Field

If you choose IP Address or MAC Address as the host type, enter the address in this field. If you choose a device type, this field is disabled.

Policy Field

If you know the name of the exception policy, enter it in this field. Click the button with three dots to the right of the Policy field to choose an existing policy or to display a dialog box in which you can create a new policy.

Choose an Exception Policy

Choose the policy that you want to apply to the host. When you choose a policy, the redirect URL specified for the policy appears in a read-only field, and the access rule entries for the policy are displayed.

If no policies are available in the list, click **Cancel** to return to the wizard screen, and then choose the option that allows you to add a policy.

Choose the policy that you want to apply to the excepted host from the list. If there are no policies in the list, click **Cancel** to return to the wizard. Then choose **Create a new policy** and choose it in the Add to the Exception List window.

Redirect URL: URL Field

This read-only field displays the redirect URL associated with the policy that you choose. Hosts to which this policy is applied are redirected to this URL when the attempt to access the network.

Preview of Access Rule

The Action, Source, Destination, and Service columns show the ACL entries in the access rule associated with the policy. These columns are empty if no ACL is configured for this policy.

Add Exception Policy

Create a new exception policy in this window.

To create a new exception policy, enter a name for the policy, and either specify an access rule that defines the IP addresses that hosts in the exception list can access, or enter a redirect URL. The redirect URL should contain remediation information that enables users to update their virus definition files. You must provide either an access rule name or a redirect URL. You can specify both.

Name Field

Enter the name for the policy in this field. Do not use question mark (?) characters or space characters in policy names. Limit each policy name to no more than 256 characters.

Access Rule Field

Enter the name of the access rule that you want to use, or click the button to the right of this field to browse for an access rule or create a new access rule. The access rule must contain permit entries that specify the IP addresses that hosts on the exception list can connect to. The access rule must be a named ACL; numbered ACLs are not supported.

Redirect URL Field

Enter a URL that contains the remediation information for your network. This information might contain instructions for downloading virus definition files.

A remediation URL might look like the following:

```
http://172.23.44.9/update
```

Redirect URLs are usually of the form `http://URL`, or `https://URL`.

Agentless Host Policy

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used as an alternative or as a complement to a NAC exception list. If you are using the NAC wizard and you do not need to configure an agentless host policy, you can click **Next** without entering information in this window.

Authenticate Agentless Hosts Check Box

Check this box to indicate that you want to use the agentless hosts policy on the Cisco Secure ACS server.

Username and Password Fields

Some Cisco IOS software images require that a username and password be supplied along with the request to the Cisco Secure ACS server. If this is required, enter the username and password configured on the Cisco Secure ACS server for this purpose. If the Cisco IOS software image does not require this information, these fields do not appear.

Configuring NAC for Remote Access

Configuring NAC for remote access allows you to modify the ACLs that NAC configuration creates so that they will permit Cisco SDM traffic. Specify the hosts that must be able to use Cisco SDM to access the router.

Enable Cisco SDM Remote Management

Check this box to enable Cisco SDM remote management on the named interface.

Host/Network Address Fields

If you want Cisco SDM to modify the ACL to allow Cisco SDM traffic from a single host, choose **Host Address** and enter the IP address of a host. Choose **Network Address** and enter the address of a network and a subnet mask to allow

Cisco SDM traffic from hosts on that network. The host or network must be accessible from the interfaces that you specified. Choose **Any** to allow Cisco SDM traffic from any host connected to the specified interfaces.

Modify Firewall

Cisco SDM checks each ACL applied to the interface specified in this configuration to determine if it blocks any traffic that should be allowed through the firewall so that the feature you are configuring will work.

Each interface is listed, along with the service currently being blocked on that interface, and the ACL that is blocking it. If you want Cisco SDM to modify the ACL to allow the traffic listed, check the **Modify** box in the appropriate row. If you want to see the entry that Cisco SDM will add to the ACL, click the **Details** button.

In the following table, FastEthernet0/0 has been configured for NAC. This interface is configured with the services shown in the Service column.

Interface	Service	ACL	Action
FastEthernet0/0	RADIUS Server	101 (INBOUND)	[ ] Modify
FastEthernet0/0	DNS	100 (INBOUND)	[ ] Modify
FastEthernet0/0	DHCP	100 (INBOUND)	[ ] Modify
FastEthernet0/0	NTP	101 (INBOUND)	[ ] Modify
FastEthernet0/0	VPN	190 (INBOUND)	[ ] Modify

Details Window

This window displays the entries that Cisco SDM will add to ACLs to allow services needed for the service you are configuring. The window might contain an entry like the following:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

In this case, web traffic whose port number is greater than 1024 is permitted from the host 10.77.158.84 on the local network to the host 10.77.158.1

Summary of the configuration

This window summarizes the information you entered, and allows you to review it in a single window. You can use the Back button to return to any wizard screen to change information. Click **Finish** to deliver the configuration to the router.

Here is an example of a NAC configuration summary:

```
NAC Interface:  FastEthernet0/1.42
Admission Name::  SDM_EOU_3


AAA Client Source Interface: FastEthernet0/1.40
NAC Policy Server 1:   10.77.158.54

Exception List
-----------------------------------------------------------------------
Address/Device     IP Address       (22.22.22.2) newly added
Policy Details:
Policy Name:        P55
      Redirect URL:  http://www.fix.com
       Access Rule:   test11


-----------------------------------------------------------------------


Enabled agentless host policy
Username:  bill
Password:    ******
```

In this example, RADIUS packets will have the IP address of FastEthernet 0/1.40. NAC is enabled on FastEthernet 0/1.42, and the NAC policy that the wizard applied is SDM_EOU_3. One host has been named in the exception list, and its access to the network is controlled by the exception policy P55.

Edit NAC Tab

The Edit NAC tab lists the NAC policies configured on the router and enables you to configure other NAC settings. A NAC policy must be configured for each interface on which posture validation is to be performed.

NAC Timeouts Button

The router and the client use Extensible Authentication Protocol over Unformatted Data Protocol (EAPoUDP) to exchange posture information. Default values for EAPoUDP timeout settings are preconfigured, but you can change the settings. This button is disabled if there is no NAC policy configured on the router.

Agentless Host Policy Button

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used when such hosts do not have static IP addresses. This button is disabled if there is no NAC policy configured on the router.

Add, Edit, and Delete Buttons

These buttons allow you to manage the NAC policy list. Click **Add** to create a new NAC policy. Use the Edit and Delete buttons to modify and remove NAC policies. The Edit and Delete buttons are disabled when no NAC policies have been configured on the router.

Only the Add button is enabled when there is no NAC policy configured on the router. The Add button is disabled when all router interfaces are configured with a NAC policy.

NAC Policies List

The name, the interface to which the NAC policy is applied, and the access rule that defines the policy are included in the list. If you enabled NAC on an interface using the Create NAC wizard, the default NAC policy SDM_EOU_1 appears in this list.

NAC Components

This window provides a brief description of the EAPoUDP components that Cisco SDM allows you to configure.

Exception List Window

This placeholder topic will be removed when the help system for NAC is built. This help topic has already been written for wizard mode. To view it, click the following link:

NAC Exception List

Exception Policies Window

NAC exception policies control the network access of hosts in the exception list. A NAC exception policy consists of a name, an access rule, and/or a redirect URL. The access rule specifies the destinations to which hosts governed by the policy have access. If a redirect URL is specified in the policy, the policy can point web clients to sites that contain information on how to obtain the latest available virus protection.

An example of a NAC policy entry is shown in the following table:

Name	Access Rule	Redirect URL
NACLess	nac-rule	http://172.30.10/update

Access rules associated with NAC policies must be extended ACLs, and must be named. An example of an access rule that might be used in a NAC policy is shown in the following table:

Action	Source	Destination	Service	Log	Attributes
permit	any	172.30.2.10	ip		

This rule permits any host governed by the policy to send IP traffic to the IP address 172.30.2.10.

Add, Edit, and Delete Buttons

Click the **Add** button to create a new exception policy. Use the **Edit** button to modify existing exception policies, and the **Delete** button to remove exception policies. The Edit and Delete buttons are disabled when there are no exception policies in the list.

NAC Timeouts

Configure the timeout values the router is to use for EAPoUDP communication with network hosts. The default, minimum, and maximum values for all settings are shown in the following table.

Value	Default	Minimum	Maximum
Hold Period Timeout	180 seconds	60 seconds	86400 seconds
Retransmission Timeout	3 seconds	1 second	60 seconds
Revalidation Timeout	36000 seconds	300 seconds	86400 seconds
Status Query Timeout	300 seconds	30 seconds	1800 seconds

Interface Selection

Choose the interface to which the NAC timeout settings are to apply.

Hold Period Timeout Field

Enter the number of seconds that the router is to ignore packets from clients that have just failed authentication.

Retransmit Timeout Field

Enter the number of seconds that the router is to wait before retransmitting EAPoUDP messages to clients.

Revalidation Timeout Field

The router periodically queries the posture agent on the client to determine the client's adherence to security policy. Enter the number of seconds that the router should wait between queries.

Status Query Timeout Field

Enter the number of seconds that the router should wait between queries to the posture agent on the host.

Reset to Defaults Button

Click this button to reset all NAC timeouts to their default values.

Configure these timeout values globally Check Box

Click this check box to have these values apply to all interfaces.

Configure a NAC Policy

A NAC policy enables the posture validation process on a router interface, and can be used to specify the types of traffic that are to be exempt from posture validation in the admission control process.

Name Field

Enter a name for the policy.

Select an Interface List

Choose the interface to which you want to apply the NAC policy. Choose an interface that connects network clients to the router.

Admission Rule Field

You can use an access rule to exempt specific traffic from triggering the admission control process. It is not required. Enter the name or the number of the access rule that you want to use for the admission rule. You can also click the button to the right of this field and browse for the access rule, or create a new access rule.

The access rule must contain deny statements that specify the traffic that is to be exempted from the admission control process. No posture validation triggering occurs if the access rule contains only deny statements.

An example of ACL entries for a NAC admission rule follows:

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any
```

The first deny statement exempts traffic with a destination of port 53 (domain), and the second statement exempts traffic with a destination of port 80 (www). The permit statement ending the ACL ensures that posture validation occurs.

How Do I...

The following topics contain procedures for performing tasks that the Create NAC wizard does not help you to do.

How Do I Configure a NAC Policy Server?

The router must have a connection to a Cisco Secure Access Control Server (ACS) running ACS software version 3.3. The ACS must be configured to use the RADIUS protocol in order to implement NAC. The document at the following link contains an overview of the configuration process.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Documents at the following link explain how to install and configure Cisco Secure ACS for Windows Servers version 3.3.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

How Do I Install and Configure a Posture Agent on a Host?

If you are a registered Cisco.com user, you can download Cisco Trust Agent (CTA) software from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

The document at the following link explains how to install and configure CTA software on a host.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

The specific installation procedures required to install third-party posture agent software and the optional remediation server vary depending on the software in use. Consult the vendor documentation for complete details.

Router Properties

Router properties let you define the overall attributes of the router, such as the router name, domain name, password, Simple Network Management Protocol (SNMP) status, Domain Name System (DNS) server address, user accounts, router log attributes, virtual type terminal (vty) settings, SSH settings, and other router access security settings.

Device Properties

The Properties—Device screen contains host, domain, and password information for your router.

Device Tab

The Device tab contains the following fields.

Host

Enter the name you want to give the router in this field.

Domain

Enter the domain name for your organization. If you do not know the domain name, obtain it from your network administrator.

Enter the Text for Banner

Enter text for the router banner. The router text banner is displayed whenever anyone logs in to the router. We recommend that the text banner include a message indicating that unauthorized access is prohibited.

Password Tab

The Password tab contains the following fields.

Enable Secret Password

Cisco Router and Security Device Manager (Cisco SDM) supports the enable secret password. The enable secret password allows you to control who is able to enter configuration commands on this router. We strongly recommend that you set an enable secret password. The password will not be readable in the Cisco SDM Device Properties window, and it will appear in encrypted form in the router configuration file. Therefore, you should record this password in case you forget it.

The Cisco IOS release that the router is running may also support the enable password. The enable password functions like the enable secret password, but was encrypted in the configuration file. If an enable password is configured using the command-line interface (CLI), it is ignored if an enable secret password is configured.

Current Password

If a password has already been set, this area contains asterisks (*).

Enter New Password

Enter the new enable password in this field.

Reenter New Password

Reenter the password exactly as you entered it in the New Password field.

Date and Time: Clock Properties

Use this window to view and edit the date and time settings on the router.

Date/Time

> You can see the router date and time settings on the right side of the Cisco SDM status bar. The time and date settings in this part of the Clock Properties window are not updated.

Router Time Source

> This field can contain the following values:

- NTP – The router receives time information from an NTP server.
- User Configuration – The time and date values are set manually, using Cisco SDM or the CLI.
- No time source – The router is not configured with time or date settings.

Change Settings

> Click to change the date and time settings on the router.

Date and Time Properties

> Use this window to set the router date and time. You can have Cisco SDM synchronize the settings with the PC, or you can set them manually.

Synchronize with my local PC clock

> Check to set up Cisco SDM to synchronize router date and time settings with the date and time settings on the PC.

Synchronize

> Click to have Cisco SDM synchronize time settings. Cisco SDM adjusts date and time settings in this way only when you click **Synchronize**. Cisco SDM does not automatically resynchronize them with the PC during subsequent sessions. This button is disabled if you have not checked **Synchronize with my local PC clock**.

> ✎
>
> **Note**   You must make the Time Zone and Daylight Savings settings on the PC before starting Cisco SDM so that Cisco SDM will receive the correct settings when you click **Synchronize**.

Edit Date and Time

Use this area to set the date and time manually. You can choose the month and the year from the drop-down lists, and choose the day of the month in the calendar. The fields in the Time area require values in 24-hour format. You can choose your time zone based on Greenwich mean time (GMT), or you can browse the list for major cities in your time zone.

If you want the router to adjust time settings for daylight saving time and standard time, check **Automatically adjust clock for daylight savings changes**.

Apply

Click to apply the date and time settings you have made in the Date, Time, and Time Zone fields.

NTP

Network Time Protocol (NTP) allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtains time and date information from a single source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, add new information, or edit or delete existing information.

> ✎
>
> **Note**   If your router does not support NTP commands, this branch will not appear in the Router Properties tree.

IP Address

The IP address of an NTP server.

If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at the following URL:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Interface

The interface over which the router will communicate with the NTP server.

Prefer

This column contains **Yes** if this NTP server has been designated as a preferred NTP server. Preferred NTP servers will be contacted before nonpreferred servers. There can be more than one preferred NTP server.

Add

Click to add NTP server information.

Edit

Click to edit a specified NTP server configuration.

Delete

Click to delete a specified NTP server configuration.

Add or Edit NTP Server Details

Add or edit NTP server information in this window.

IP Address

Enter or edit the IP address of an NTP server.

Prefer

Click this box if this is to be the preferred NTP server.

Interface

Choose the router interface that will provide access to the NTP server. You can use the **show IP routes** CLI command to determine which interface has a route to this NTP server.

✎
Note An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule is already in place for this interface, Cisco SDM will add statements to permit port 123 traffic on this interface. If the existing rule is a standard access rule, Cisco SDM changes it to an extended rule in order to be able to specify traffic type and destination.

Authentication Key

Check this box if the NTP server uses an authentication key, and enter the information required in the fields. The information in these fields must match the key information on the NTP server.

Key Number

Enter the number for the authentication key. The key number range is 0 to 4294967295.

Key Value

Enter the key used by the NTP server. The key value can use any of the letters A to Z, uppercase or lowercase, and can be no more than 32 characters.

Confirm Key Value

Reenter the key value to confirm accuracy.

SNTP

This window is displayed on Cisco 830 routers. The Simple Network Time Protocol (SNTP) is a less complex version of Network Time Protocol (NTP). NTP allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single

source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, to add new information, or to edit or delete existing information.

> ✎
>
> **Note**   If your router does not support NTP commands, this branch will not appear in the Router Properties tree.

Property

The system-defined name for this NTP server.

Value

The IP address for this NTP server.

Add

Click to add NTP server information.

Edit

Click to edit a specified NTP server configuration.

Delete

Click to delete a specified NTP server configuration.

Add an NTP Server

Enter the IP address of an NTP server in this window.

> ✎
>
> **Note**   An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule was already in place for this interface, Cisco SDM will add statements to permit port 123 traffic on this interface. If the existing rule was a standard access rule, Cisco SDM changes it to an extended rule in order to be able to specify traffic type and destination.

IP Address

Enter the IP address of the NTP server in dotted-decimal format. For more information, see IP Addresses and Subnet Masks.

Logging

Use this window to enable logging of system messages, and to specify logging hosts where logs can be kept. You can specify the level of logging messages that you want to send and to collect, and enter the hostname or IP address of multiple logging hosts.

IP Address/Hostname

Click **Add**, and enter the IP address or hostname of a network host to which you want the router to send logging messages for storage. The **Edit** and **Delete** buttons enable you to modify information that you entered and to delete entries.

Specify the types of messages that are sent to logging hosts by choosing the logging level from the **Logging Level** drop-down list. See Logging Level for more information.

Logging Level

The following logging levels are available in **Logging Level** drop-down lists:

- emergencies (0)
- alerts (1)
- critical (2)
- errors (3)
- warnings (4)
- notifications (5)
- informational (6)
- debugging (7)

The log collects all messages of the level you choose plus all messages of lower levels, or the router sends all messages of the level you choose plus all messages of lower levels to the logging hosts. For example, if you choose notifications (5),

the log collects or sends messages of levels 0 through 5. Firewall logging
messages require a logging level of debugging(7), and Application Security
logging messages require a level of informational(6).

Logging to Buffer

If you want system messages to be logged to the router buffer, check the **Logging
Buffer** check box in the dialog that Cisco SDM displays when you click **Edit**,
then enter the buffer size in the Buffer Size field. The larger the buffer, the more
entries can be stored before the oldest ones are deleted to make room for new
entries. However, you should balance logging needs against router performance.

Specify the types of messages that are collected in the log by choosing the logging
level from the **Logging Level** drop-down list. See Logging Level for more
information.

SNMP

This window lets you enable SNMP, set SNMP community strings, and enter
SNMP trap manager information.

Enable SNMP

Check this check box to enable SNMP support. Uncheck to disable SNMP
support. SNMP is enabled by default.

Community String

SNMP community strings are embedded passwords to Management Information
Bases (MIBs). MIBs store data about router operation and are meant to be
available to authenticated remote users. The two types of community strings are
"public" community strings, which provide read-only access to all objects in the
MIB except community strings, and "private" community strings, which provide
read-and-write access to all objects in the MIB except community strings.

The community string table lists all of the configured community strings and their
types. Use the **Add** button to display the Add a Community String dialog box and
create new community strings. Click the **Edit** or **Delete** buttons to edit or delete
the community string you chose in the table.

Trap Receiver

Enter the IP addresses and community strings of the trap receivers—that is, the addresses where the trap information should be sent. These are normally the IP addresses of the SNMP management stations monitoring your domain. Check with your site administrator to determine the address if you are unsure of it.

Click the **Add**, **Edit**, or **Delete** buttons to administer trap receiver information.

SNMP Server Location

Text field you can use to enter the SNMP server location. It is not a configuration parameter that will affect the operation of the router.

SNMP Server Contact

Text field you can use to enter contact information for a person managing the SNMP server. It is not a configuration parameter that will affect the operation of the router.

Netflow

This window shows how your router is configured to monitor Netflow top talkers on interfaces that have Netflow configured. For more information on the items shown, see Netflow Talkers.

You can monitor Netflow parameters on your router and view top-talker statistics in **Monitor > Inteface Status** and **Monitor > Traffic Status > Top N Traffic Flows**. If you do *not* enable Netflow top talkers, then the top ten talkers are monitored.

Netflow Talkers

In this window you can Netflow top talkers.

Enable Top Talkers

Check the **Enable Top Talkers** check box to enable monitoring of the top talkers on the interfaces that have Netflow configured.

Top Talkers

> Set the number of top talkers in the **Top Talkers** number box. Choose a number in the range 1–200. Cisco SDM will track and record data on up to the number of top talkers that you set.

Cache Timeout

> Set the timeout, in milliseconds, for the top-talkers cache in the **Cache timeout** number box. Choose a number in the range 1–3600000. The top-talkers cache will refresh when the timeout is reached.

Sort By

> Choose how to sort the top talkers by choosing bytes or packets from the **Sort by** drop-down list.

Router Access

> This window explains which features are included in router access.

User Accounts: Configure User Accounts for Router Access

> This window allows you to define accounts and passwords that will enable users to authenticate themselves when logging in to the router using HTTP, Telnet, PPP, or some other means.

Username

> User account name.

Password

> User account password, displayed as asterisks (*).

> **Note** The user password is not the same as the enable secret password configured in the Device Properties—Password tab. The user password enables the specified user to log in to the router and enter a limited set of commands.

Privilege Level

Privilege level for the user.

View Name

If a CLI view has been associated with the user account, the view name appears in this column. Views define the user's access to Cisco SDM based on the user's role. Click Associate a View with the user for more information.

> **Note** If Cisco SDM is launched with a user-defined view, or with an altered Cisco SDM-defined view, Cisco SDM operates in Monitor mode, and the user has read-only privileges. The Cisco SDM features available to be monitored depend on the commands present in the view. Not all features may be available for monitoring by the user.

What Do You Want To Do?

To:	Do This:
Add a new user account.	Click **Add**. Then add the account in the Add a Username window.
Edit a user account.	Choose the user account and click **Edit**. Then edit the account in the Edit a Username window.
Delete a user account.	Choose the user account and click **Delete**. Then, confirm the deletion in the displayed warning box.

Add or Edit a Username

Add or edit a user account in the fields provided in this window.

Username

Enter or edit the username in this field.

Password

Enter or edit the password in this field.

Confirm Password

Reenter the password in this field. If the password and the confirm password do not match, an error message window appears when you click **OK**.

When you click **OK**, the new or edited account information appears in the Configure User Accounts for Telnet window.

Encrypt password using MD5 hash algorithm Check Box

Check if you want the password to be encrypted using the one-way Message Digest 5 (MD5) algorithm, which provides strong encryption protection.

> **Note** Protocols that require the retrieval of clear text passwords, such as CHAP, cannot be used with MD5-encrypted passwords. MD5 encryption is not reversible. To restore the password to clear text, you must delete the user account and re-create it without checking the **Encrypt password** option.

Privilege Level

Enter the privilege level for the user. When applied to a CLI command, that command can only be executed by users with a privilege level equal to or higher than the level set for the command.

Associate a View with the user

This field is displayed when you are setting up user accounts for router access. It may not be visible if you are working in a different area of Cisco SDM.

Check the **Associate a View with the user** option if you want to restrict user access to a specific view. If you associate a view with any user for the first time, you are prompted to enter the view password. This option is only available in the Router Access node of the Additional Tasks tree.

View Name:

Choose the view you want to associate with this user from the following:

- SDM_Administrator—A user associated with the view type SDM_Administrator has complete access to Cisco SDM and can perform all operations supported by Cisco SDM.

- SDM_Monitor—A user associated with the view type SDM_Monitor can monitor all features supported by Cisco SDM. The user is not able to deliver configurations using Cisco SDM. The user is able to navigate the various areas of Cisco SDM, such as Interfaces and Connections, Firewall, and VPN. However, the user interface components in these areas are disabled.

- SDM_Firewall—A user associated with the view type SDM_Firewall can use the Cisco SDM Firewall and Monitor features. The user can configure firewalls and ACLs using the Firewall wizard, Firewall Policy View, and ACL Editor. User interface components in other areas are disabled for this user.

- SDM_EasyVPN_Remote—A user associated with the view type SDM_EasyVPN_Remote can use the Cisco SDM Easy VPN Remote features. The user is able to create Easy VPN Remote connections and edit them. User interface components in other areas are disabled for this user.

Details

The **Associate a View for this user** area displays details of the specified view. Click the **Details** button for a more detailed information about the specified view.

View Password

When you associate a view with any user for the first time, you are prompted to enter the view password for Cisco SDM-defined views. Use this password to switch between other views.

Enter the View Password

Enter the view password in the View Password field.

vty Settings

This window displays the virtual terminal (vty) settings on your router. The Property column contains configured line ranges and configurable properties for each range. The settings for these properties are contained in the Value column.

This table shows your router vty settings and contains the following columns:

- Line Range—Displays the range of vty connections to which the rest of the settings in the row apply.

- Input Protocols Allowed—Shows the protocols configured for input. Can be Telnet, SSH, or both Telnet and SSH.

- Output Protocols Allowed—Shows the protocols configured for output. Can be Telnet, SSH, or both Telnet and SSH.

- EXEC Timeout—Number of seconds of inactivity after which a session is terminated.

- Inbound Access-class—Name or number of the access rule applied to the inbound direction of the line range.

- Outbound Access-class—Name or number of the access rule applied to the outbound direction of the line range.

- ACL—If configured, shows the ACL associated with the vty connections.

- Authentication Policy—The AAA authentication policy associated with this vty line. This field is visible if AAA is configured on the router.

- Authorization Policy—The AAA authorization policy associated with this vty line. This field is visible if AAA is configured on the router.

Note To use SSH as an input or output protocol, you must enable it by clicking **SSH** in the Additional Tasks tree and generating an RSA key.

Edit vty Lines

This window lets you edit virtual terminal (vty) settings on your router.

Line Range

Enter the range of vty lines to which the settings made in this window will apply.

Time Out

Enter the number of seconds of inactivity allowed to pass before an inactive connection will be terminated.

Input Protocol

Choose the input protocols by clicking the appropriate check boxes.

Telnet Check Box

Check to enableTelnet access to your router.

SSH Check Box

Check to enable SSH clients to log in to the router.

Output Protocol

Choose the output protocols by clicking the appropriate check boxes.

Telnet Check Box

Check to enable Telnet access to your router.

SSH Check Box

Check to enable the router to communicate with SSH clients.

Access Rule

You can associate access rules to filter inbound and outbound traffic on the vty lines in the range.

Inbound

Enter the name or number of the access rule you want to filter inbound traffic, or click the button and browse for the access rule.

Outbound

Enter the name or number of the access rule you want to filter outbound traffic, or click the button and browse for the access rule.

Authentication/Authorization

These fields are visible when AAA is enabled on the router. AAA can be enabled by clicking **Additional Tasks** > **AAA** > **Enable**.

Authentication Policy

Choose the authentication policy that you want to use for this vty line.

Authorization Policy

Choose the authorization policy that you want to use for this vty line.

Configure Management Access Policies

Use this window to review existing management access policies and to choose policies for editing. Management access policies specify which networks and hosts will be able to access the router command-line interface. In the policy, you can specify which protocols the host or network in the policy can use, and which router interface will carry the management traffic.

Host/Network

A network address or host IP address. If a network address is given, the policy applies to all hosts on that network. If a host address is given, the policy applies to that host.

A network address is shown in the format network number/network bits, as in the following example:

```
172.23.44.0/24
```

For more information on this format, and on how IP addresses and subnet masks are used, see IP Addresses and Subnet Masks.

Management Interface

The router interface over which management traffic will flow.

Permitted Protocols

This column lists the protocols that the specified hosts can use when communicating with the router. The following protocols can be configured:

- Cisco SDM—Specified hosts can use Cisco SDM.

- Telnet—Specified hosts can use Telnet to access the router CLI.

- SSH—Specified hosts can use Secure Shell to access the router CLI.

- HTTP—Specified hosts can use Hypertext Transfer Protocol to access the router. If Cisco SDM is specified, either HTTP or HTTPS must also be specified.

- HTTPS—Specified hosts can use Hypertext Transfer Protocol Secure to access the router.

- RCP—Specified hosts can use Remote Copy Protocol to manage files on the router.

- SNMP—Specified hosts can use Simple Network Management Protocol to manage the router.

Add Button

Click to add a management policy, and specify the policy in the Add a Management Policy window.

Edit Button

Click to edit a management policy, and specify the policy in the Edit a Management Policy window.

Delete Button

Click to delete a specified management policy.

Apply Button

Click to apply changes you made in the Add or Edit a Management Policy window to the router configuration.

Discard Changes Button

Click to discard changes you made in the Add or Edit a Management Policy window to the router configuration. The changes you made are discarded and removed from the Configure Management Access Policies window.

Add or Edit a Management Policy

Use this window to add or edit a management policy.

Type

Specify whether the address you provide is the address of a host or a network.

IP Address/Subnet Mask

If you specified **Network** in the Type field, enter the IP address of a host, or the network address and subnet mask. For more information, see IP Addresses and Subnet Masks.

Interface

Choose the interface through which you want to allow management traffic. The interface should be the most direct route from the host or network to the local router.

Management Protocols

Specify the management protocols allowed for the host or network.

Allow SDM

Check to allow the specified host or network to access Cisco SDM. When you check this box, the following protocols are automatically checked: Telnet, SSH, HTTP, HTTPS, and RCP. Checking this option does not prevent you from allowing additional protocols.

If you want to make users employ secure protocols when logging in to Cisco SDM, check **Allow secure protocols only**. When you check this box, the following protocols are automatically checked: SSH, HTTPS, RCP. If you then check a nonsecure protocol such as Telnet, Cisco SDM unchecks **Allow secure protocols only**.

You Can Specify Management Protocols Individually

If you want to specify individual protocols that the host or network can use, you can check any of the boxes: Telnet, SSH, HTTP, RCP, or SNMP.

If Telnet and SSH are not enabled (checked) in the VTYs window, and SNMP is not enabled in the SNMP Properties window, Cisco SDM will advise you to enable those protocols when they are specified in this window.

Note   The options **Allow secure protocols only** and **HTTPS** are disabled if the Cisco IOS release on the router does not support HTTPS.

Management Access Error Messages

The following error messages may be generated by the Management Access feature.

Error Message

SDM Warning: ANY Not Allowed

> **Explanation**   A management policy is read-only if any of its source or destination rule entries contain the "any" keyword. Such policies cannot be edited in the Management Access window. A policy containing the "any" keyword can create a security risk for the following reasons:
>
> – If "any" is associated with source, it allows traffic from any network to enter the router.

– If "any" is associated with destination, it allows access to any node on the network supported by the router.

Recommended Action You can remove the access entry that caused this message to appear by choosing the rule in the Rules window and clicking **Edit**. Alternatively, in the Interfaces and Connections window, you can disassociate the rule from the interface it is applied to.

Error Message

```
SDM Warning: Unsupported Access Control Entry
```

Explanation A management policy will be read only if unsupported access control entries (ACEs) are associated with the interface or vty line to which you applied the management policy. You can use the CLI to remove the unsupported ACEs. Unsupported ACEs are those that contain keywords or syntax that Cisco SDM does not support.

Error Message

```
SDM Warning: SDM Not Allowed
```

Explanation This message is displayed if you still have not configured a management access policy to allow a host or network to access Cisco SDM on this router.

Recommended Action You must provide such a policy in order to make Cisco SDM on this router accessible. You cannot navigate to other features or deliver commands to the router until you configure a management access policy to allow access to Cisco SDM for a host or network.

Error Message

SDM Warning: Current Host Not Allowed

Explanation This message is displayed if you have not configured a management access policy to allow the current host or network to access Cisco SDM on this router.

Recommended Action You should create such a policy in order to make Cisco SDM on this router accessible from the current host or network. If you do not, you will lose the connection to the router when you deliver the configuration to the router. Click **Yes** to add to a management access policy now for the current host or network. Click **No** to proceed without adding a policy for the current host or network. You will lose contact with the router during command delivery, and you will have to log in to Cisco SDM using a different host or network.

SSH

This router implements Secure Shell (SSH) Server, a feature that enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality similar to that of an inbound Telnet connection, but which provides strong encryption to be used with Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients. This feature is disabled if the router is not using an IPsec DES or 3DES Cisco IOS release, and if the SSH branch of the Additional Tasks tree does not appear.

SSH uses an RSA cryptographic key to encrypt data traveling between the router and the SSH client. Generating the RSA key in this window enables SSH communication between the router and the SSH clients.

Status Messages

Crypto key is not set on this device

Appears if there is no cryptographic key configured for the device. If there is no key configured, you can enter a modulus size and generate a key.

RSA key is set on this router

Appears if a cryptographic key was generated. SSH is enabled on this router.

Key modulus size Button

Visible if no cryptographic key has been generated. Click this button and enter the modulus size you want to give the key. If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

Generate RSA Key Button

Click to generate a cryptographic key for the router using the modulus size you entered. If the cryptographic key was generated, this button is disabled.

DHCP Configuration

This window explains how you can manage DHCP configurations on your router.

DHCP Pools

This window displays the DHCP pools configured on the router.

Pool Name

The name of the DHCP pool.

Interface

The interface on which the DHCP pool is configured. Clients attached to this interface will receive IP addresses from this DHCP pool.

Details of DHCP Pool *name*

This area provides the following details about the pool identified in *name*:

- **DHCP Pool Range**—Range of IP addresses that can be granted to clients.

- **Default Router IP Address**—If the router has an IP address in the same subnet as the DHCP pool, it is shown here.

- **DNS Servers**—IP addresses of the DNS servers that the router will provide to DHCP clients.

- **WINS Servers**—IP addresses of the WINS servers that the router will provide to DHCP clients.

- **Domain Name**—Domain name configured on the router.

- **Lease Time**—Amount of time that the router will lease an IP address to a client.

- **Import All**—Whether the router imports DHCP option parameters to the DHCP server database and also sends this information to DHCP clients on the LAN when they request IP addresses.

Add

Choose this option to create a new DHCP pool. The user must specify the DHCP pool name, DHCP pool network, DHCP pool IP address range, and lease time. Optionally, DNS servers, WINS server, the domain name, and the default router can also be configured in the DHCP pool.

Edit

Choose this option to edit an existing DHCP pool.

Delete

Choose this option to delete a DHCP pool.

DHCP Pool Status

Click this button to see the IP addresses leased by the specified pool. If a DHCP pool contains any parameters other than pool network, IP address range, lease time, DNS servers, WINS servers, domain name, and default router, Cisco SDM shows this pool as read-only. If a pool contains a discontinuous range of IP addresses, it also is shown as read-only.

Add or Edit DHCP Pool

Add or edit a DHCP pool in this window. You cannot edit Cisco SDM-default pools.

DHCP Pool Name

Provide a name for the DHCP pool in this field.

DHCP Pool Network

Enter the network from which the IP addresses in the pool will be taken, for example, 192.168.233.0. This cannot be the IP address of an individual host.

Subnet Mask

Enter the subnet mask. The subnet mask of 255.255.255.0 provides 255 IP addresses.

DHCP Pool

Enter the starting and ending IP addresses in the range. For example, if the network is 192.168.233.0 and the subnet mask is 255.255.255.0, the starting address is 192.168.233.1 and the ending address is 192.168.233.254.

Lease Length

Enter the amount of time that addresses are to be leased to clients. You can specify that leased addresses never expire, or you can specify the lease time in days, hours, and minutes. Do not exceed 365 days, 23 hours, or 59 minutes.

DHCP Options

Enter information for the DNS servers, WINS servers, the domain name, and the default router in the DHCP options fields. These values are sent to DHCP clients when they request an IP address.

Import all DHCP Options into the DHCP server database

Click this option if you want to import DHCP option parameters into the DHCP server database and also send this information to DHCP clients on the LAN when they request IP addresses.

DHCP Bindings

This window shows existing manual DHCP bindings. A manual DHCP binding allows you to allocate the same IP address to a specific client each time the client requests an IP address from the available DHCP pools.

You can also add new bindings, edit existing bindings, or delete existing bindings.

Binding Name

Name assigned to the DHCP binding.

Host/IP Mask

IP address and mask bound to the client.

MAC Address

MAC address of the client.

Type

Type of MAC address is one of the following:

- Ethernet

  Client has a hardware address.

- IEEE802

  Client has a hardware address.

- <None>

  Client has a client identifier.

Client Name

Optional name assigned to the client.

Add Button

Click to add a new manual DHCP binding.

Edit Button

Click to edit the specified manual DHCP binding.

Delete Button

Click to delete the specified manual DHCP binding.

Add or Edit DHCP Binding

This window allows you to add or edit existing manual DHCP bindings.

Name

Enter the name you want for the DHCP binding. If you are editing the DHCP binding, the name field is read-only.

Host IP

Enter the IP address you want to bind to the client. The address should be from the DHCP pool available to the client. Do not enter an address in use by another DHCP binding.

Mask

Enter the mask used for the host IP address.

Identifier

From the drop-down menu, choose a method for identifying the client with a MAC address.

MAC Address

Enter the MAC address of the client. Do not enter an address in use by another DHCP binding.

Type

If you chose **Hardware Address** from the Identifier drop-down menu, choose **Ethernet** or **IEEE802** to set the MAC address type of the client.

Client Name (Optional)

Enter a name to identify the client. The name should be a hostname only, not a domain-style name. For example, *router* is an acceptable name, but *router.cisco.com* is not.

DNS Properties

The Domain Name System (DNS) is a database of Internet hostnames with their corresponding IP addresses distributed over designated DNS servers. It enables network users to refer to hosts by name, rather than by IP addresses, which are harder to remember. Use this window to enable the use of DNS servers for hostname-to-address translation.

Enable DNS-based hostname to address translation Check Box

Check to enable the router to use DNS. Uncheck if you do not want to use DNS.

DNS IP Address

Enter the IP addresses of the DNS servers that you want the router to send DNS requests to.

Click the **Add**, **Edit**, or **Delete** buttons to administer DNS IP address information.

Dynamic DNS Methods

This window shows a list of dynamic DNS methods.

Each dynamic DNS method shown will send with its update the hostname and domain name configured in **Configure > Additional Tasks > Router Properties**. However, if you create a dynamic DNS method when configuring a WAN interface, you can override the hostname and domain name configured in **Configure > Additional Tasks > Router Properties**. The new hostname and domain name will apply only to that dynamic DNS method.

Some dynamic DNS methods are read-only. These were configured in the Cisco IOS software through the CLI, and cannot be edited or deleted. To make these read-only methods editable, use the CLI to change the internal cache or host group options to HTTP or IETF.

Add Button

Click the **Add** button to create a new dynamic DNS method.

Edit Button

To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Edit**.

Delete Button

To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Delete**.

Note   A warning appears if you attempt to delete a dynamic DNS method that is associated with one or more interfaces.

Add or Edit Dynamic DNS Method

This window allows you to add or edit a dynamic DNS method. Set the type of method by choosing **HTTP** or **IETF**.

HTTP

HTTP is a dynamic DNS method type that updates a DNS service provider with changes to the associated interface's IP address.

Server

If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.

Username

If using HTTP, enter a username for accessing the DNS service provider.

Password

If using HTTP, enter a password for accessing the DNS service provider.

IETF

IETF is a dynamic DNS method type that updates a DNS server with changes to the associated interface's IP address.

If using IETF, configure a DNS server for the router in **Configure > Additional Tasks > DNS**.

ACL Editor

Rules define how the router will respond to a particular kind of traffic. Using Cisco SDM, you can create access rules that cause the router to block certain types of traffic while permitting other types, NAT rules that define the traffic that is to receive address translation, and IPSec rules that specify which traffic is to be encrypted. Cisco SDM also provides default rules that are used in guided configurations, and that you can examine and use when you create your own access rules. It also allows you to view rules that were not created using Cisco SDM, called external rules, and rules with syntax that Cisco SDM does not support, called unsupported rules.

Use the Rules screen to view a summary of the rules in the router's configuration and to navigate to other windows to create, edit, or delete rules.

Category

A type of rule. One of the following:

Access Rules	Rules that govern the traffic that can enter and leave the network. These rules are used by router interfaces, and by VTY lines that let users log on to the router.
NAT Rules	Rules that determine how private IP addresses are translated into valid Internet IP addresses.
IPSec Rules	Rules that determine which traffic will be encrypted on secure connections.

NAC Rules	Rules that specify the IP addresses to be admitted to the network, or blocked from the network.
Firewall Rules	Rules that can specify source and destination addresses, type of traffic, and whether the traffic should be permitted or denied.
QoS Rules	Rules that specify traffic that should belong to the QoS Class that the rule is associated with.
Unsupported Rules	Rules that have not been created using Cisco SDM, and that Cisco SDM does not support. These rules are read only, and cannot be modified using Cisco SDM.
Externally Defined Rules	Rules that have not been created using Cisco SDM, but that Cisco SDM does support. These rules may not be associated with any interface.
Cisco SDM Default Rules	These rules are predefined rules that are used by Cisco SDM wizards and that you can apply in the Additional Tasks>ACL Editor windows.

No. of Rules

The number of rules of this type.

Description

A description of the rule if one has been entered.

To configure rules:

Click the category of rule in the rule tree to display the window for that type of rule. Create and edit rules from that window.

The help topic for these windows contains general procedures that you may find helpful. Useful Procedures for Access Rules and Firewalls contains step by step procedures for other tasks.

Useful Procedures for Access Rules and Firewalls

This section contains procedures that you may find useful.

- How Do I View Activity on My Firewall?
- How Do I Configure a Firewall on an Unsupported Interface?
- How Do I Configure a Firewall After I Have Configured a VPN?
- How Do I Permit Specific Traffic Through a DMZ Interface?
- How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?
- How Do I Configure NAT Passthrough for a Firewall?
- How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?
- How Do I Associate a Rule with an Interface?
- How Do I Disassociate an Access Rule from an Interface
- How Do I Delete a Rule That Is Associated with an Interface?
- How Do I Create an Access Rule for a Java List?

Rules Windows

These windows let you examine, create, edit, and delete rules.

- Access Rules window—Access rules most commonly define the traffic that you want to permit or deny entry to your LAN or exit from your LAN, but they can be used for other purposes as well.
- NAT Rules window—NAT rules are used to specify a set of addresses to translate.
- IPSec Rules window—IPSec rules are extended rules used in IPSec policies to specify which traffic will be encrypted for VPN connections.
- NAC Rules window—Rules that specify the IP addresses to be admitted to the network, or blocked from the network.
- Firewall Rules window—Rules that can specify source and destination addresses, type of traffic, and whether the traffic should be permitted or denied.

- QoS Rules window—Rules that specify traffic that should belong to the QoS Class that the rule is associated with.

- Unsupported Rules window—Unsupported rules contain syntax or keywords that Cisco SDM does not support. Unsupported rules may affect the way the router operates, but are marked as read-only by Cisco SDM.

- Externally Defined Rules window—Externally defined rules are those that Cisco SDM was not used to create.

- Cisco SDM Default Rules window—Cisco SDM default rules are pre-defined access rules. They are used in guided first-time configurations, and you can use them in configurations that you create.

- NAC Rules window. NAC rules are used in the NAC exception policy to specify hosts that are to be exempted from the NAC validation process. They are also used to define the hosts or networks for admission control.

The upper portion of the screen lists the access rules that have been configured on this router. This list does not contain Cisco SDM default rules. To view Cisco SDM default rules, click the **SDM Default Rules** branch of the Rules tree.

The lower portion of the window lists the rule entries associated with the selected rule. A rule entry consists of criteria that incoming or outgoing traffic is compared against, and the action to take on traffic matching the criteria. If traffic does not match the criteria of any of the entries in this box, it is dropped.

First column

This column may contain icons that indicate the status of a rule.

If the rule is read only, the read-only icon will appear in this column.

Name/Number

The name or the number of the access rule.

The numbers 1 through 99 are used to identify standard access lists. The numbers 100 through 199 are used to identify extended access lists. Names, which can contain alphabetic characters, allow you to extend the range of standard access lists beyond 99, and extended access lists beyond 199.

Used By

The name of the interface or VTY numbers to which this rule has been applied.

Type

The type of rule, either standard or extended.

Standard rules compare a packet's source IP address against its IP address criteria to determine a match. The rule's IP address criteria can be a single IP address, or portions of an IP address, defined by a wildcard mask.

Extended rules can examine a greater variety of packet fields to determine a match. Extended rules can examine both the packet's source and destination IP addresses, the protocol type, the source and destination ports, and other packet fields.

Access rules can be either standard rules or extended rules. IPSec rules have to extended rules because they must be able to specify a service type. Externally defined and unsupported rules may be either standard or extended.

Description

A description of the rule, if one has been entered.

First Column (Rule Entry Area)

✔   Permit traffic.

❌   Deny traffic.

Action

The action to take when a packet matching the criteria in this entry arrives on the interface. Either Permit or Deny:

- Permit—Allow traffic matching the criteria in this row.

- Deny—Do not allow traffic matching the criteria in this row.

Click Meanings of the Permit and Deny Keywords to learn more about the action of permit and the action of deny in the context of a specific type of rule.

Source

The source IP address criteria that the traffic must match. This column may contain:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address

- A host name.

Destination

For extended rules, the destination IP address criteria that the traffic must match. The address may be for a network, or a specific host. This column may contain:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address

- A host name.

Service

For extended rules, the service specifies the type of traffic that packets matching the rule must contain. This is shown by displaying the service, such as echo-reply, followed by the protocol, such as ICMP. A rule permitting or denying multiple services between the same end points must contain an entry for each service.

Attributes

This field can contain other information about this entry, such as whether logging has been enabled.

Description

A short description of the entry.

What do you want to do?

If you want to:	Do this:
Add a rule.	Click the **Add** button and create the rule in the windows displayed.
Edit a rule, or edit a rule entry.	Select the access rule and click **Edit**. Then edit the rule in the Edit rule window displayed.
Associate a rule with an interface.	See How Do I Associate a Rule with an Interface?
Delete a rule that has not been associated with an interface.	Select the Access rule, and click **Delete**.
Delete a rule that has been associated with an interface	Cisco SDM does not permit you to delete a rule that has been associated with an interface. In order to delete the rule, you must first disassociate it from the interface. See How Do I Delete a Rule That Is Associated with an Interface?
What I want to do is not described here.	The following link contains procedures that you may want to consult: Useful Procedures for Access Rules and Firewalls.

Add or Edit a Rule

This window lets you add or edit a rule you have selected in the Rules window. You can rename or renumber the rule, add, change, reorder, or delete rule entries, and add or change the description of the rule.

Name/Number

Add or edit the name or number of the rule.

Standard rules must be numbered in the range 1–99, or 1300–1999.

Extended rules must be numbered in the range 100–199 or 2000–2699.

Names, which can contain alphabetic characters, allow you to associate a meaningful label to the access rule.

Type

Select the type of rule you are adding. Standard rules let you have the router examine the source host or network in the packet. Extended rules let you have the router examine the source host or network, the destination host or network, and the type of traffic that the packet contains.

Description

You can provide a description of the rule in this field. The description must be less than 100 characters long.

Rule Entry List

This list shows the entries that make up the rule. You can add, edit, and delete entries. You can also reorder them to change the order in which they are evaluated.

Observe the following guidelines when creating rule entries:

- There must be at least one permit statement in the list; otherwise, all traffic will be denied.

- A permit all or deny all entry in the list must be the last entry.

- Standard entries and extended entries cannot be mixed in the same rule.

- No duplicate entries can exist in the same rule.

Clone

Click this button to use the selected entry as a template for a new entry. This feature can save you time, and help reduce errors. For example, if you want to create a number of extended rule entries with the same source and destination, but different protocols or ports, you could create the first one using the Add button. After creating the first entry, you could copy it using **Clone**, and change the protocol field or port field to create a new entry.

Interface Association

Click the **Associate** button to apply the rule to an interface.

Note   The Associate button is enabled only if you are adding a rule from the Access
Rules window.

What do you want to do?

If you want to:	Do this:
Add or edit a rule entry.	Click **Add,** and create the entry in the window displayed. Or click **Edit**, and change the entry in the window displayed.
Add a rule entry using an existing entry as a template.	Select the entry you want to use as a template, and click **Clone**. Then create the entry in the dialog box displayed. The dialog box displays the contents of the entry you selected so that you can edit it to create a new entry.
Reorder rule entries to make sure that the router evaluates particular entries.	Select the rule entry, and click the **Move Up** or the **Move Down** button to move the entry where you want it.
Associate a rule with an interface.	Click **Associate** and select the interface and direction in the Associate with an Interface window. If the **Associate** button is not enabled, you can associate the rule with an interface by double-clicking the interface in the Interfaces and Connections window and using the Associate tab.
Delete a rule entry.	Select the rule entry, and click **Delete**. Then confirm deletion in the Warning window displayed.
Learn more about rules.	Explore the resources on Cisco.com. The following link contains information about IP access lists: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml
What I want to do is not described here.	The following link contains procedures that you may want to consult: Useful Procedures for Access Rules and Firewalls

Associate with an Interface

You can use this window to associate a rule you have created from the Access Rules window with an interface and to specify whether it applies to outbound traffic or inbound traffic.

Select an Interface

Select the interface to which you want this rule to apply.

Specify a Direction

If you want the router to check packets inbound to the interface, click **Inbound**. The router checks for a match with the rule before routing it; the router accepts or drops the packet based on whether the rule states permit or deny. If you want the router to forward the packet to the outbound interface before comparing it to the entries in the access rule, click **Outbound**.

If Another Rule is Already Associated with the Interface

If an information box appears that tells that another Access Rule is associated with the interface and direction you specified, you can either cancel the operation, or you can continue, by appending the rule entries to the rule that is already applied to the interface, or by disassociating the rule with the interface and associating the new rule.

What do you want to do?

If you want to:	Do this:
Cancel the operation and preserve the association between the interface and the existing rule.	Click **No**. The association between the existing rule and the interface is preserved, and the rule that you created in the Add a Rule window is saved.
	You can examine the existing rule and the new rule and decide whether you want to replace the existing rule or to merge the entries of the new rule with the existing rule.
Continue, and merge the entries of the rule you created with the entries of the existing rule.	Click **Yes**. Then, when the window appears that asks whether you want to merge or replace the existing rule, click **Merge**.
	The entries you created for the new rule are appended after the last entry of the existing rule.
	✎ **Note** If the rule you want to merge is not compatible with the existing rule, you will be allowed only to replace the existing rule.
Continue, and replace the rule existing rule with the rule you created.	Click **Yes**. Then, when the window appears that asks you if you want to merge or replace the existing rule, click **Replace**.
	The rule you are replacing is not erased. It is just disassociated with the interface and direction.

Add a Standard Rule Entry

A standard rule entry allows you to permit or deny traffic that came from a specified source. The source can be a network or a host within a specific network. You can create a single rule entry in this window, but you can return to this window to create additional entries for a rule if you need to.

> **Note** Any traffic that does not match the criteria in one of the rule entries you create is implicitly denied. To ensure that traffic you do not intend to deny is permitted, you must append explicit permit entries to the that rule you are configuring.

Action

Select the action you want the router to take when a packet matches the criteria in the rule entry. The choices are **Permit** and **Deny**. What Permit and Deny do depends on the type of rule in which they are used. In Cisco SDM, standard rule entries can be used in access rules, NAT rules, and in access lists associated with route maps. Click Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A Network. Select if you want the action to apply to all the IP addresses in a network.

- A Host Name or IP Address. Select if you want the action to apply to a specificc host or IP address.

- Any IP address. Select if you want the action to apply to any IP address.

IP Address

If you selected **A Network or if you selected A Host Name or IP address**, enter the IP address in this field. If the address you enter is a network address, enter a wildcard mask to specify the parts of the network address that must be matched.

Mask

If you selected **A Network or if you selected A Host Name or IP address**, either select the wildcard mask from this list, or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in a packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname/IP

If you selected **A Host Name or IP address** in the Type field, enter the name oro the IP address of the host. If you enter a hostname, the router must be configured to use a DNS server.

Description

You can enter a short description of the entry in this field. The description must be fewer than 100 characters long.

Log Matches Against This Entry

If you have specified syslog in System Properties, you can check this box; matches will be recorded in the system log.

Add an Extended Rule Entry

An extended rule entry allows you to permit or deny traffic based on its source and destination and on the protocol and service specified in the packet.

> **Note**   Any traffic that does not match the criteria in one of the rule entries you create is implicitly denied. To ensure that traffic you do not intend to deny is permitted, you must append explicit permit entries to the rule that you are configuring.

Action

Select the action you want the router to take when a packet matches the criteria in the rule entry. The choices are **Permit** and **Deny**. If you are creating an entry for an IPSec rule, the choices are **protect the traffic** and **don't protect the traffic**.

What Permit and Deny do depends on the type of rule in which they are used. In Cisco SDM, extended rule entries can be used in access rules, NAT rules, IPSec rules, and access lists associated with route maps. Click Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A specific IP address. This can be a network address, or the address of a specific host.

- A host name.

- Any IP address.

IP Address

If you selected **A specific IP address**, enter the **IP address** in this field. If the address you enter is a network address, enter a wildcard mask to specify the parts of the network address that must be matched.

Mask

If you selected **A specific IP address**, either select the wildcard mask from this list, or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in the packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname

If you selected **A host name** in the Type field, enter the name of the host.

Destination Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A specific IP address. This can be a network address or the address of a specific host.
- A host name.
- Any IP address.

Mask

If you selected **A specific IP address**, either select the wildcard mask from this list or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in the packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname

If you selected **A host name** in the Type field, enter the name of the host.

Description

You can enter a short description of the entry in this field. The description must be fewer than 100 characters long.

Protocol and Service

Select the protocol and service, if applicable, that you want the entry to apply to. The information that you provide differs from protocol to protocol. Click the protocol to see what information you need to provide.

Source Port

Available when either TCP or UDP is selected. Setting this field will cause the router to filter on the source port in a packet. It is rarely necessary to set a source port value for a TCP connection. If you are not sure you need to use this field, leave it set to **= any**.

Destination Port

Available when either TCP or UDP is selected. Setting this field will cause the router to filter on the destination port in a packet.

If you select this protocol:	You can specify the following in the Source Port and Destination Port fields:
TCP and UDP	Specify the source and destination port by name or number. If you do not remember the name or number, click the **...** button and select the value you want from the Service window. This field accepts protocol numbers from 0 through 65535. • =. The rule entry applies to the value that you enter in the field to the right. • !=. The rule entry applies to any value except the one that you enter in the field to the right. • <. The rule entry applies to all port numbers lower than the number you enter. • >. The rule entry applies to all port numbers higher than the number you enter. • range. The entry applies to the range of port numbers that you specify in the fields to the right.
ICMP	Specify **any** ICMP type, or specify a type by name or number. If you do not remember the name or number, click the **...** button, and select the value you want. This field accepts protocol numbers from 0 through 255.
IP	Specify **any** IP protocol, or specify a protocol by name or number. If you do not remember the name or number, click the **...** button, and select the value you want. This field accepts protocol numbers from 0 through 255.

See Services and Ports to see a table containing port names and numbers available in Cisco SDM.

Log Matches Against This Entry

If you have configured logging for firewall messages, you can check this box and matches will be recorded in the log file sent to the syslog server. For more information refer to this link: Firewall Log.

Select a Rule

Use this window to select a rule to use.

Rule Category

Select the rule category that you want to select from. The rules in the category you select will appear in the box below the list. If no rules appear in the box, no rules of that category have been defined.

Name/Number

The name or number of the rule.

Used By

How the rule is being used. For example, if the rule has been associated with an interface, the name of the interface. If the rule is being used in an IPSec policy, the name of the policy. Or, if the rule has been used by NAT, this column contains the value NAT.

Description

A description of the rule.

Preview

This area of the screen displays the entries of the selected rule.

Action

Either **Permit** or **Deny**. See Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source

The source IP address criteria that the traffic must match. This column may contain the following:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address

- A host name.

Destination

For extended rules, the destination IP address criteria that the traffic must match. The address may be for a network, or a specific host. This column may contain the following:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address

- A host name.

Service

For extended rules, the service specifies the type of traffic that packets matching the rule must contain. This is shown by displaying the service, such as echo-reply, followed by the protocol, such as ICMP. A rule permitting or denying multiple services between the same endpoints must contain an entry for each service.

Port-to-Application Mapping

Port-to-Application Mapping (PAM) allows you to customize TCP and UDP port numbers for network services and applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

The information that PAM maintains enables Context-Based Access Control (CBAC) supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

Port-to-Application Mappings

This window displays the port-to-application mappings configured on the router and allows you to add, edit and remove PAM entries. Each row in the window displays a PAM entry, and entries are grouped according to type.

Add, Edit, and Delete Buttons

Use these buttons to create, edit, or remove PAM entries. Clicking the **Add** button lets you create entries that map nonstandard port numbers to protocol names. Clicking the **Edit** button lets you make changes to user-defined entries. Entries with the value *System Defined* in the Protocol Type column cannot be edited or deleted.

Application Protocol Column

This column contains the name of the application protocol, and the names of the protocol types. For example, the FTP and the TFTP entries are found under the File Transfer protocol type.

Port Type Column

This list appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic.

Port Column

This column contains the port number. For example the system-defined entry for HTTP would have the port number 80 in this column. A user-defined entry for HTTP might have the port number 8080 or another custom-defined number in this column.

Protocol Type Column

A row in this column displays one of the following values:

- **User-Defined**—The entry contains a nonstandard mapping between a protocol and protocol number. The entry could be associated with a host IP address identified by the access control list (ACL) whose number is displayed in the Access List column.

- **System-Defined**—The entry contains a standard, registered mapping between the protocol and protocol number, such as *tftp 69*, or *smtp 25*. System-defined entries cannot be edited or deleted. System-defined entries contain no value in the Access List column because they apply to all hosts on the network.

Access List Column

A PAM entry applies to a single host, defined by a standard ACL. This column displays the number of the ACL used to identify the host to which the PAM entry applies. If you want to view the ACL that identifies the host, go to **Additional Tasks > ACL Editor > Access Rules**. Then click the number of the ACL that you saw in this window.

Description Column

If a description of the PAM entry has been created, the description is displayed in this column.

Add or Edit Port Map Entry

You can add and edit port map entries for custom or standard protocols.

Protocol Field

If you are adding an entry, specify the protocol by clicking the list (**...**) button to the right and choosing a system-defined protocol, or by entering the name of a custom protocol. You cannot enter custom-defined protocol names for which a port mapping already exists.

If you are editing an entry, the protocol field is disabled. If you need to change the protocol, delete the PAM entry and re-create it using the protocol information that you need.

Description Field

This field appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic. You can optionally enter a description of the port map entry. Descriptions are helpful when you are adding entries for custom protocols or special applications. For example, if you created an entry for a custom database application named "orville" running on host sf-5, you might enter "orville-sf-5."

Port Type List

This list appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic. Choose either **TCP** or **UDP**. The default is TCP.

Port Number Field

Enter the port number that you want to map to the protocol that you specified. If the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic, you can enter multiple port

numbers separated by commas, or port number ranges indicated with a dash. For example, you might enter three noncontiguous port numbers as 310, 313, 318, or you might enter the range 415–419.

If the router is not running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic, you can enter a single port number.

Host of Service Field

Specify the IP address of the host to which this port mapping is to apply. If you need the same mapping for another host, create a separate PAM entry for that host.

Zone-Based Policy Firewall

Zone-based policy firewall (also known as "Zone-Policy Firewall" or "ZPF") changes the firewall from the older interface-based model to a more flexible, more easily understood zone-based configuration model. Interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface.

Firewall policies are configured with the Cisco Common Classification Policy Language (C3PL), which employs a hierarchical structure to define inspection for network protocols and the groups of hosts to which the inspection will be applied.

For a good description of how Zone- Based Policy Firewall can be implemented, read *The Zone-Based Policy Firewall Design Guide* available on cisco.com by going to **Support > Product Support > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Configure > Feature Guides** and clicking Zone-Based Policy Firewall Design Guide. This document may also be available at the following link:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Configuration Task Order

The following task order can be followed to configure a Zone-Based Policy Firewall:

1. Define zones.

2. Define zone-pairs.

3. Define class-maps that describe traffic that must have policy applied as it crosses a zone-pair.

4. Define policy-maps to apply action to your class-map's traffic.

5. Apply policy-maps to zone-pairs.

6. Assign interfaces to zones.

The sequence of tasks is not important, but some events must be completed in order. For instance, you must configure a class-map before you assign a class-map to a policy-map. Similarly, you cannot assign a policy-map to a zone-pair until you have configured the policy. If you try to complete a task that relies on another portion of the configuration that you have not configured, SDM does not allow you to do so.

Zone Window

A zone, or security zone, is a group of interfaces to which a security policy can be applied. The interfaces in a zone should share common functions or features. For example, two interfaces that are connected to the local LAN might be placed in one security zone, and the interfaces connected to the Internet might be placed in another security zone.

For traffic to flow among all the interfaces in a router, all the interfaces must be a member of one security zone or another. It is not necessary for all router interfaces to be members of security zones.

Zone-based Policy General Rules describes the rules governing interface behavior and the flow of traffic between zone-member interfaces.

This window displays the name of each security zone, the interfaces that it contains, and any associated zone pairs that the zone is a member of. A zone can be a member of multiple zone pairs.

Click **Add** to create a new zone.

Click **Edit** to choose different interfaces for an existing zone.

Click **Delete** to remove a zone. A zone that is a member of a zone pair cannot be deleted.

Add or Edit a Zone

To add a new zone, also called a security zone, enter a zone name, and choose the interfaces that are to be included in the zone. The Interface list displays the names of available interfaces. Because physical interfaces can be placed in only one zone, they do not appear in the list if they have already been placed in a zone. Virtual interfaces, such as Dialer interfaces or Virtual Template interfaces can be placed in multiple zones and will always appear in the list.

Note
- Traffic flowing to or from this interface is governed by the policy map associated with the zone.

- An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, SDM does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.

  – Go to **Configure > Firewall and ACL > Edit Firewall Policy > Rule for New Traffic**. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select **Permit ACL**.

  – Go to **Configure > C3PL > Policy Map > Protocol Inspection**. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

After a zone has been created, you can change the interfaces associated with the zone, but you cannot change the name of the zone.

Zone-Based Policy General Rules

Router network interfaces' membership in zones is subject to several rules governing interface behavior, as is the traffic moving between zone member interfaces:

- A zone must be configured before interfaces can be assigned to the zone.

- An interface can be assigned to only one security zone.

- All traffic to/from a given interface is implicitly blocked when the interface is assigned to a zone, excepting traffic to/from other interfaces in the same zone, and traffic to any interface on the router.

- Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

- To permit traffic to/from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

- The self zone is the only exception to the default deny-all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

- Traffic cannot flow between a zone member interface and any interface that is not a zone member.

- Pass, inspect, and drop actions can only be applied between two zones.

- Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.

- If it is required that an interface on the box not be part of the zoning/firewall policy, it might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.

- From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).

- The only exception to the preceding deny by default approach is the traffic to/from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

This set of rules was taken from *The Zone-Based Policy Firewall Design Guide* available at the following link:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Zone Pairs

A zone-pair allows you to specify a unidirectional firewall policy between two security zones. The direction of the traffic is specified by specifying a source and destination security zone.The same zone cannot be defined as both the source and the destination.

If you want traffic to flow in both directions between two zones, you must create a zone pair for each direction. If you want traffic to flow freely among all interfaces, each interface must be configured in a zone.

The following table shows an example of four zone-pairs.

Zone Pair	Source	Destination	Policy
LAN-out	zone-VLAN1	zone-FE1	inspection-policymap-a
LAN-in	zone-FE1	zone-VLAN1	inspection-policymap-b
Bkup-out	self	zone-BRI0	inspection-policymap-c
Bkup-in	zone-BRI0	self	inspection-policymap-c

LAN-out and LAN-in are zone-pairs configured for traffic flowing between the LAN interface, VLAN1, and the FastEthernet 1 interface. Each zone-pair is controlled by a separate policy. Bkup-out and Bkup-in are configured for traffic generated by the router. The same policy controls traffic sent from zone-BRI0 as traffic sent by the router, represented by the self zone.

Click **Add** to create a zone-pair.

Click **Edit** to change the policy associated with a zone pair.

Click **Delete** to remove a zone pair.

Add or Edit a Zone Pair

To configure a new zone pair, provide a name for the zone pair, a source zone from which traffic will originate, a destination zone to which traffic is to be sent, and the policy that is to determine which traffic can be sent across the zones. The source zone and destination zone lists contain the zones configured on the router and the self zone. The self zone can be used when you are configuring zone pairs

for traffic originating from the router itself, or destined for the router itself, such as a zone pair configured for SNMP traffic. The Policy list contains the name of each policy map configured on the router.

If you are editing a zone pair, you can change the policy map, but you cannot change the name or the source or destination zones.

Add a Zone

You can configure an interface as a member of a security zone from the Association tab of the Edit Interfaces and Connections dialog. The zone that you add will include the interface that you are editing as a zone member.

Note
- Traffic flowing to or from this interface is governed by the policy map associated with the zone.

- An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, SDM does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.

  – Go to **Configure > Firewall and ACL > Edit Firewall Policy > Rule for New Traffic**. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select **Permit ACL**.

  – Go to **Configure > C3PL > Policy Map > Protocol Inspection**. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

Zone Name

Enter the name of the zone that you want to add.

Select a Zone

If a security zone has been configured on the router, you can add the interface that you are configuring as a member of that zone.

Select a Zone for the Interface

Select the zone that you want to include the interface in, and click **OK**.

Zone Pairs

Authentication, Authorization, and Accounting

Cisco IOS Authentication, Authorization, and Accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco IOS AAA provides the following benefits:

- Increased flexibility and control
- Scalability
- Standardized authentication methods. Cisco SDM enables you to configure the Remote Authentication Dialin User Service (RADIUS), and the Terminal Access Controller Access Control System Plus (TACACS+) authentication methods.

This chapter contains the following section:

- Configuring AAA
- AAA Screen Reference

Configuring AAA

To configure AAA, complete the following steps:

Step 1   If you want to review the IOS CLI commands that you send to the router when you complete the configuration, go to the Cisco SDM toolbar, and click **Edit > Preferences > Preview commands before delivering to router**. The preview screen allows you to cancel the configuration if you want to.

Step 2   In the Cisco SDM toolbar, click **Configure**.

Step 3   In the Cisco SDM taskbar, click **Additional Tasks**.

Step 4   In the Additional Tasks tree, click **AAA**.

Step 5   In the AAA screen, click **Enable AAA**. This enables AAA on the router.

Step 6   Click **+** (the plus sign) next to the AAA folder to display other AAA branches.

Step 7   Click the branch for the type of configuration you need to perform.

Step 8   In the displayed AAA screen, click **Add** to create a configuration, or select an existing entry in the screen, and click **Edit** to change configuration settings.

Step 9   Make configuration settings in the displayed dialogs, and click **OK** to send the configuration to the router. If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **OK** to send the configuration to the router, or click **Cancel** to discard it.

AAA Screen Reference

The topics in this section describe the AAA configuration screens:

- AAA Root Screen
- AAA Servers and Server Groups
- AAA Servers
- Add or Edit a TACACS+ Server
- Add or Edit a RADIUS Server

- AAA Server Groups
- Add or Edit AAA Server Group
- Authentication and Authorization Policies
- Authentication and Authorization
- Authentication NAC
- Authentication 802.1x
- Add or Edit a Method List for Authentication or Authorization

AAA Root Screen

This screen is located at the top level of the AAA tree. It provides a summary view of the AAA configuration on the router. To view more detailed information or to edit the AAA configuration, click the appropriate node on the AAA tree.

Field Reference

Table 35-12 describes the fields in this screen.

Table 35-1   AAA Main Screen Fields

Element	Description
Enable AAA Disable AAA	If AAA is enabled, the button name is Disable AAA. If AAA is disabled, the button name is Enable AAA. AAA is enabled by default. If you click **Disable AAA**, Cisco SDM displays a message telling you that it will make configuration changes to ensure that the router can be accessed. Disabling AAA will prevent you from configuring your router as an Easy VPN server, and will prevent you from associating user accounts with command line interface (CLI) views.
AAA Servers and Groups	This read-only field displays a count of the AAA servers and server groups. The router relays authentication, authorization, and accounting requests to AAA servers. AAA servers are organized into groups to provide the router with alternate servers to contact if the first server contacted is not available.

Table 35-1   AAA Main Screen Fields

Element	Description
Authentication Policies	This read-only field lists configured authentication policies. Authentication policies define how users are identified. To edit authentication policies, click the **Login** sub-node under **Authentication Policies** in the AAA tree.
Authorization Policies	This read-only field lists configured authorization policies. Authorization policies define the methods that are used to permit or deny a user login. To edit authorization policies, click **Authorization Policies** in the AAA tree.
	To edit authorization policies (Exec Authorization and Network Authorization), click the **Exec** and **Network** sub-nodes respectively under the **Authorization Policies** node in the AAA tree.

AAA Servers and Server Groups

This window provides a description of AAA servers and AAA server groups.

To display the AAA Servers window, click the **AAA Servers** branch.

To display the AAA Server Groups window, click the **AAA Server Groups** branch.

AAA Servers

This window lets you view a snapshot of the information about the AAA servers that the router is configured to use. The IP address, server type, and other parameters are displayed for each server.

Field Reference

Table 35-2 describes the fields in this screen.

Table 35-2   AAA Servers Fields

Element	Description
Global Settings	Click **Global Settings** to make global settings for TACACS+ and RADIUS servers. In the Edit Global Settings window, you can specify how long to attempt contact with an AAA server before going on to the next server, the key to use when contacting TACACS+ or RADIUS servers, and the interface on which TACACS+ or RADIUS packets will be received. These settings will apply to all servers for which server-specific settings have not been made.
Add	Click **Add** to add a TACACS+ or a RADIUS server to the list.
Edit	Click **Edit** to edit the information for the selected AAA server.
Delete	Click **Delete** to delete the information for the selected AAA server.
Server IP	The IP address of the AAA server.
Parameters	This column lists the timeout, key, and other parameters for each server.

Add or Edit a TACACS+ Server

Add or edit information for a TACACS+ server in this window.

Field Reference

Table 35-3 describes the fields in this screen.

Table 35-3   Add or Edit a TACACS+ Server Fields

Element	Description
Server IP or Host	Enter the IP address or the host name of the server. If the router has not been configured to use a Domain Name Service (DNS) server, enter an IP address.
Single Connection to Server	Check this box if you want the router to maintain a single open connection to the TACACS+ server, rather than opening and closing a TCP connection each time it communicates with the server. A single open connection is more efficient because it allows the TACACS+ server to handle a higher number of TACACS+ operations.
	✎
	Note This option is supported only if the TACACS+ server is running CiscoSecure version 1.0.1 or later.
Server-specific setup	Check **Server-specific setup** if you want to override AAA server global settings, and specify a server-specific timeout value and encryption key. You can make the following settings:
	• Timeout (seconds)—Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window.
	• Configure Key—Optional. Enter the key to use to encrypt traffic between the router and this server. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window.
	• New Key/Confirm Key—Enter the key and reenter it for confirmation.

Add or Edit a RADIUS Server

Add or edit information for a RADIUS server in this window.

Field Reference

Table 35-4 describes the fields in this screen.

Table 35-4   Add or Edit a RADIUS Server Fields

Element	Description
Server IP or Host	Enter the IP address or the host name of the server. If the router has not been configured to use a Domain Name Service (DNS) server, enter an IP address.
Authorization Port	Specify the server port to use for authorization requests. The default is 1645.
Accounting Port	Specify the server port to use for accounting requests. The default is 1646.
Timeout in seconds	Optional. Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window.
Configure Key	Optional. Enter the key to use to encrypt traffic between the router and this server. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window. • New Key and Confirm Key—Enter the key and reenter it for confirmation.

Edit Global Settings

You can specify communication settings that will apply to all communications between the router and AAA servers in this window. Any communications settings made for a specific router will override settings made in this window.

Field Reference

Table 35-12 describes the fields in this screen.

Table 35-5   Global Settings Fields

Element	Description
TACACS+ Server RADIUS Server	Click the appropriate button to specify the server type for which you are setting global parameters. If you select TACACS+ Server, the parameters will apply to all communication with TACACS+ servers that do not have server specific parameters set. If you select RADIUS Server, the parameters will apply to all communication with RADIUS servers that do not have server specific parameters set.
Timeout (seconds)	Enter the number of seconds to wait for a response from the RADIUS or TACACS+ server
Key	Enter the encryption key for all communication between the router and the TACACS+ or RADIUS servers.
Select the source interface	Check this box if you want to specify a single interface on which the router is to receive TACACS+ or RADIUS packets. Interface—Select the router interface on which the router is to receive TACACS+ or RADIUS packets.If the **Select the source interface** box is not checked, this field will be disabled.

AAA Server Groups

This window displays the AAA server groups configured on this router. If no AAA servers have been configured, this window is empty.

Field Reference

Table 35-6 describes the fields in this screen.

Table 35-6   AAA Server Groups Fields

Element	Description
Add	Click the **Add** button to create a RADIUS server group. After you create this group, the name and group members are displayed in this window.
Edit	Click **Edit** to modify the information for the highlighted server group.
Delete	Click **Delete** to remove the highlighted server group.
Group Name	The name of the server group. Server group names allow you to use a single name to reference multiple servers.
Type	The type of servers in the selected group, either TACACS+, or RADIUS.
Group Members	The IP addresses or host names of the AAA servers in this group.

Add or Edit AAA Server Group

Create or modify an AAA server group in this window.

Field Reference

Table 35-7 describes the fields in this screen.

Table 35-7   Add or Edit AAA Server Group Fields

Element	Description
Group Name	Enter a name for the group.

Table 35-7   Add or Edit AAA Server Group Fields

Element	Description
Server Type	Select the Server type, either RADIUS, or TACACS+. ✎ **Note** This field may be protected and set to a specific type, depending on the configuration that you are performing.
Select the servers that need to be placed in this AAA server group	This area lists the IP addresses of all the AAA servers configured on the router of the type chosen, along with the Authorization and Accounting ports used. Check the **Select** box next to the servers that you want to add.

Authentication and Authorization Policies

The Authentication Policies and the Authorization Policies windows summarize the authentication policy information on the router.

Field Reference

Table 35-8 describes the fields in this screen.

Table 35-8   Authentication and Authorization Policy Fields

Element	Description
Authentication Type	The type of authentication policy.
Number of Policies	The number of policies of this type.
Usage	The usage description for these policies.

Authentication and Authorization

The Login and the Exec and Network authorization windows display the method lists used to authenticate logins, NAC requests and authorize Exec command level and network requests. You can review and manage these method lists from these windows.

Field Reference

Table 35-9 describes the fields in this screen.

Table 35-9   Authentication and Authorization Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user.
Method 1	The method that the router will attempt first. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods, in order, that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Authentication NAC

The Authentication NAC window displays the EAPoUDP method lists configured on the router. You can specify additional method lists in this window if you want the router to attempt the methods that you enter before resorting to the default method list.

Field Reference

Table 35-10 describes the fields in this screen.

Table 35-10   NAC Authentication Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. If the NAC wizard was used to create a NAC configuration, the list name "default" is displayed in this column.
Method 1	The method that the router will attempt first. If the NAC wizard was used to create a NAC configuration, the method name "group SDM_NAC_Group" is displayed in this column. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods, in order, that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Authentication 802.1x

The Authentication 802.1x window displays the method lists configured for 802.1x authentication.

Note   You cannot specify additional method lists for 802.1x configuration.

Field Reference

Table 35-11 describes the fields in this screen.

Table 35-11   802.1x Authentication Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. If the LAN wizard has been used to create an 802.1x configuration, the list name "default" is displayed in this column.
Method 1	The method that the router will attempt first. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list. If the LAN wizard has been used to create an 802.1x configuration, the Method name "group SDM_802.1x" is displayed in this column.
Method 2 Method 3 Method 4	The methods that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Add or Edit a Method List for Authentication or Authorization

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails.

Cisco IOS software uses the first listed method to authenticate users. If that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

It is important to note that the Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

Field Reference

Table 35-12 describes the fields in this screen.

Table 35-12   Add a Method List for Authentication or Authorization Fields

Element	Description
Name Specify	Choose the name **Default** in the Name list, or choose **User Defined**, and enter a method list name in the Specify field.
Methods	A method is a configured server group. Up to four methods can be specified and placed in the list in the order you want the router to use them. The router will attempt the first method in the list. If the authentication request receives a PASS or a FAIL response, the router does not query further. If the router does not receive a response by using the first method, it uses the next method in the list, and continues to the end of the list until it receives a PASS or a FAIL response.
Add	Click **Add** to add a method to the list. If there are no configured server groups to add, you can configure a server group in the window displayed.
Delete	Click this button to delete a method from the list.

Table 35-12   Add a Method List for Authentication or Authorization Fields

Element	Description
Move Up Move Down	The router attempts the methods in the order they are listed in this window. Click **Move Up** to move a method up the list. Click **Move Down** to move a method further down the list. The method "none" will always be last in the list. No other method in the list can be moved below it. This is an IOS restriction. IOS will not accept any method name after the method name "none" has been added to a Method List.
Enable Password Aging	Check **Enable Password Aging** to have the Easy VPN Server notify the user when their password has expired and prompt them to enter a new password.

Router Provisioning

You can provision your router using a USB device attached directly to your router, or using Secure Device Provisioning (SDP). SDP must be supported by your Cisco IOS release to be available in Cisco SDM.

Secure Device Provisioning

This window allows you to use Secure Device Provisioning (SDP) to complete tasks such as enrolling your router with a CA server and configuring your router. Click the **Launch SDP** button to transfer to the SDP web-browser application to complete the process.

If you are obtaining certificates, Cisco SDM displays the Certificates window where you can view the certificates after they are obtained from the CA.

To learn what you need to do to prepare for SDP enrollment, see SDP Troubleshooting Tips.

For more information on SDP, click the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

Note If the **Launch SDP** button is absent, you router Cisco IOS release does not support SDP. If the **Launch SDP** button is disabled, you are logged in to Cisco SDM as a nonroot view user.

Router Provisioning from USB

This window tells you if Cisco SDM has detected a USB token or USB flash device connected to your router. You can click the **Router Provisioning** button to choose a configuration file from the USB token or USB flash device.

If you choose to provision your router this way, the configuration file from the USB token or USB flash device is merged with your router's running configuration file to create a new running configuration file.

Router Provisioning from USB (Load File)

This window allows you to load a configuration file from a USB token or USB flash device connected to your router. The file will be merged with your router's running configuration file to create a new running configuration file.

To load a configuration file, follow these steps:

Step 1   Choose the device type from the drop-down menu.

Step 2   Enter the configuration filename in Filename, including the full path, or click **Browse** and choose the file from the File Selection window.

Step 3   If the device type is a USB token, enter the password to log in to the token in Token PIN.

Step 4   If you want to preview the file, click **Preview File** to display the contents of the file in the details pane.

Step 5   Click **OK** to load the chosen file.

SDP Troubleshooting Tips

Use this information before enrolling using Secure Device Provisioning (SDP) to prepare the connection between the router and the certificate server. If you experience problems enrolling, you can review these tasks to determine where the problem is.

Guidelines

- When SDP is launched, you must minimize the browser window displaying this help topic so that you can view the SDP web application.

- If you are planning to configure the router using SDP, you should do so immediately after configuring your WAN connection.

- When you complete the configuration changes in SDP, you must return to Cisco SDM and click Refresh on the toolbar to view the status of the trustpoint in the Router Certificates window in the VPN Components tree.

Troubleshooting Tips

These recommendations involve preparations on the local router and on the CA server. You need to communicate these requirements to the administrator of the CA server. Ensure the following:

- The local router and the CA server have IP connectivity between each other. The local router must be able to ping the certificate server successfully, and the certificate server must be able to successfully ping the local router.

- The CA server administrator uses a web browser that supports JavaScript.

- The CA server administrator has enable privileges on the local router.

- The firewall on the local router will permit traffic to and from the certificate server.

- If a firewall is configured on the Petitioner and/or on the Registrar, you must ensure that the Firewall permits HTTP or HTTPS traffic from the PC from which the Cisco SDM /SDP application is invoked.

For more information about SDP, see the following web page:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

■ SDP Troubleshooting Tips

Cisco Common Classification Policy Language

Cisco Common Classification Policy Language (C3PL) is a structured replacement for feature-specific configuration commands. C3PL allows you to create traffic policies based on events, conditions, and actions. Cisco Router and Security Device Manager (Cisco SDM) uses C3PL to create the policy maps and class maps that the following help topics describe.

Policy Map

Policy maps specify the actions to be taken when traffic matches defined criteria. Traffic types and criteria are defined in class maps associated with a policy map. In order for a router to use the information in a policy map and its associated class maps, the policy map must be associated with a zone-pair. See Zone-Based Policy Firewall for more information on configuring zones and zone pairs.

Policy Map Windows

Use the policy map windows to review, create and edit policy maps for QoS, HTTP, and other types of traffic. The top portion of the window lists the configured policy maps, and the bottom portion displays the details of the highlighted policy map. If you need to edit a policy map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

This help topic provides a general description for the policy map windows and some sample data.

Add

Click **Add** to display a dialog in which you can configure a policy map.

Edit

Click **Edit** to display a dialog in which you can edit the selected policy map. The **Edit** button is disabled if no policy maps have been configured.

Delete

Click **Delete** to remove the selected policy map.

Policy Map List Area

This area lists the policy maps configured for the particular protocol or feature. Select a policy map to display details in the lower part of the screen. The following example shows two IM policies.

Policy Map Name	Description
im-pmap-g	guest policy
im-pmap-e	employee policy

Details of Policy Map

The details of the selected policy map shows the policy map configuration. The detail shown varies according to the type of policy map.

HTTP, IM, P2P, IMAP, and POP3 display a match class name, action and log column. The following table shows detail for an IM policy map. The router blocks AOL traffic, but allows all other types of IM traffic.

Match Class Name	Action	Log
aol-cmap	Disabled	Disabled
class-default	Enabled	Disabled

Protocol Inspection, SMTP, and SUNRPC policy map detail includes Match Class Name and Action columns.The following table shows detail for a SUNRPC policy map.

Match Class Name	Action
cmap-sunrpc1	Allow
cmap-sunrpc2	None

Add or Edit a QoS Policy Map

Use this information as you add or edit a QoS policy map.

Policy Name and Description

If you are creating a new policy map, enter a name and a description for it in these fields. If you are editing a policy map, these fields are display only.

Class Map, Queuing, Set DSCP, and Drop

These columns summarize the information about each class map in the policy map. The following example entry is for a voice class map:

```
Voice-FastEthernet0/1 LLQ 70%    ef         No
```

This class map uses low latency queuing, and 70% of the bandwidth for this interface. The DSCP value is set to ef, and packets of this type are not dropped.

Click the **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons to modify the class map information in this list.

Associate a Policy Map to Interface

In this screen, associate a policy map to the chosen interface.

Field Reference

Table 37-1 describes the fields in this screen.

Table 37-1   Associate a Policy Map Fields

Element	Description
Policy Map	Choose the policy map that you want to associate with the interface.
Policy Map details	
Class Map	The Class Map column displays the class maps that the policy map contains.

Queuing	The Queuing column displays the type of queuing used by the class map, and the percentage of bandwidth allocated to the class. For example, the Queuing column might contain the following entries:
	
	`LLQ - 33%`
	`CBWFQ - 5%`
	`CBWFQ - 5% Remaining`
	`Fair Queue`
	
	One class map uses Low Latency Queuing (LLQ), two class maps use Class-Based Weighted Fair Queuing (CBWFQ), and one uses Fair Queuing. The percentages show the bandwidth, or remaining bandwidth allocated to these class maps.

Shaping	The Shaping column indicates whether shaping is configured for the class map or not. • Yes—Shaping is configured. • No—Shaping is not configured.
Policing	The Shaping column indicates whether policing is configured for the class map or not. • Yes—Policing is configured. • No—Policing is not configured.
Set DSCP	The Set DSCP column lists the DSCP markings used in the class map.
Drop	

Add an Inspection Policy Map

Inspection policy maps specify the action that the router will take for traffic that matches the criteria in the associated class maps. The router can allow the traffic to pass, can drop the traffic and optionally log the event, or can inspect the traffic.

The name and description that you enter will be visible in the Inspect Policy Maps window. The Class Map and Action columns display the class maps associated with this policy map, and the action that the router will take for the traffic that the class map describes. Click **Add** to add a new class map to the list and configure the action. Click **Edit** to modify the settings for a class map. Click the the **Move Up**, and **Move Down** buttons to change the order in which the class maps are evaluated.

Layer 7 Policy Map

This window allows you to select a Layer 7 Policy map to use to inspect an application that you have selected. The window displays the policy maps available for that application. Choose a policy map and click **OK**.

Application Inspection

Application inspection policies are applied at Layer 7 of the Open Systems Interconnect (OSI) model, where user applications send and receive messages that allow the applications to offer useful capabilities. Some applications might offer undesired or vulnerable capabilities, so the messages associated with these capabilities must be filtered to limit activities on the application services.

Cisco IOS Software Zone-Policy Firewall offers application inspection and control on the following application services: HTTP, SMTP, POP3, IMAP, SUNRPC, P2P, and IMAP applications. See the following links for more information

- Add an HTTP Inspection Class Map
- Add or Edit an SMTP Class Map
- Add or Edit a POP3 Class Map
- Add or Edit an IMAP Class Map
- Add or Edit a SUNRPC Class Map

- Add or Edit a Point-to-Point Class Map
- Add or Edit an Instant Messaging Class Map

Configure Deep Packet Inspection

Layer 7 (application) inspection augments Layer 4 inspection with the capability to recognize and apply service-specific actions, such as selectively blocking or allowing file search, file transfer, and text chat capabilities. Service-specific capabilities vary by service.

If you are creating a new policy map, enter a name in the **Policy Map Name** field. You can also add a description. Click **Add > New Class Map** to create a new Point-to-Point class map. Add or Edit a Point-to-Point Class Map provides information on how to create this type of class map. Click **Add > class default** to add the default class map.

When the class map appears in the table, specify the action that you want taken when a match is found, and whether you want matches logged. You can specify **<None>**, **Reset**, or **Allow**. In the following example, there are P2P class maps for gnutella and eDonkey.

Match Class Name	Action	Log
gnutellaCMap	Allow	
eDonkeyCMap	Reset	X

Class Maps

Class maps define the traffic that a Zone-Policy Based Firewall (ZPF) selects for policy application. Layer 4 class maps sort the traffic based on the following criteria:

- Access group—A standard, extended, or named Access Control List can filter traffic based on source and destination IP address and on source and destination port.
- Protocol—The Layer 4 protocols (TCP, UDP, and ICMP) and application services such as HTTP, SMTP, DNS, etc. Any well-known or user-defined service known to PAM may be specified.

- Class map—A subordinate class map providing additional match criteria can be nested inside another class map.

Class Maps can apply "match any" or "match all" operators to determine how to apply the match criteria. If "match any" is specified, traffic must meet only one of the match criteria in the class map. If "match all" is specified, traffic must match all of the class map's criteria to belong to that particular class.

Associate Class Map

To associate a class map with an inspect policy map, complete the following tasks.

Step 1   Specify a class map name by clicking the button to the right of the name field and choosing **Add a Class Map**, **Select a Class Map**, or **class-default**.

Step 2   In the Action box, click **Pass**, **Drop**, or **Inspect**. If you click Drop, you can optionally click **Log** to have the drop event logged. If you click Inspect, click **Advanced Options** to specify the parameter maps, inspection policies, or policing that you want for the traffic in this class.

Step 3   Click **OK** to close this dialog and return to the Add dialog or the Edit an Inspection Policy Map dialog.

Class Map Advanced Options

When you choose the inspect action for traffic, you can specify parameter maps, application inspection, and ZPF policing.

Inspect Parameter Map

Inspect parameter maps specify TCP, DNS, and UDP timeouts and session control parameters. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

URL Filtering Parameter Map

URL filtering parameter maps can specify URL filtering servers and local URL lists. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

Enable Application Inspection

An application inspection policy specifies the types of data to inspect in packets of a specified application. You can select an existing application inspection policy. If no application inspection policy is configured, this field is disabled. Click **View** to display the selected application inspection policy without leaving this dialog.

Police Rate and Burst

You can limit traffic to a specified police rate and specify a burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The burst rate can be a value between 1,000 and 512,000,000 bytes.

QoS Class Map

Use this window to display and edit QoS class map information. QoS class maps are used in QoS policy maps to define types of traffic.

Click a class map name to display details about that class map in the Details of Class Map area.

The details of a class map show which protocols are matched to define the traffic. The following example shows details of a voice signaling class map.

```
Details of Class Map:SDMSignal-FastEthernet0/1

    Item Name                        Item Value
Match Protocols                      h323,rtcp
```

H.323 and RTCP are the voice signaling protocols to be matched.

Add or Edit a QoS Class Map

Use this information to help add or edit a QoS class map. If you are adding a new QoS class map, click the button on the right of the field and choose either **Add a Classmap** or **Select a Classmap** from the context menu.

See the information in Action to learn about the Drop, Set DSCP, and Queuing options.

Add or Edit a QoS Class Map

Enter a name and description of the QoS class Map you are creating so that it can be easily identified and used. Click Classification for a description of the Any, All, and Edit buttons in the Classification box.

Select a Class Map

Click the name of the class map that you want to choose, and click **OK**. The class map entry is added to the window from which you invoked this dialog.

Deep Inspection

Deep inspection allows you to create class maps for parameters specific to an application. For example, you can create class maps for the common P2P applications such as eDonkey, gnutella, and kazaa2.

Class Map and Application Service Group Windows

Use the class map windows to review, create, and edit class maps for protocols such as HTTP, SMTP, and POP3. The Class Map area of the window lists the configured class maps, and the bottom part displays the details for the selected class map. To edit a class map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

Add

Click **Add** to create a new class map of the type you have selected and enter the configuration in the displayed dialog.

Edit

Click **Edit** to change the configuration of the selected class map.

Delete

Click **Delete** to remove the selected class map. Cisco SDM may display dialogs if there are dependencies associated with this configuration, such as subordinate class maps or parameter maps that could be used by other class maps.

Class Map Area

This area displays the class maps configured for the protocol that you selected. It contains the names of the configured class maps and other relevant information.

QoS Class Maps

QoS class maps are displayed in a table with a Class Map Name and a Description column. A sample table follows.

Class Map Name	Description
CMAP-DMZ	FTP and HTTP QoS class map
CMAP-3	Test

Inspection, HTTP, SMTP, SUN RPC, IMAP and POP3 Class Maps

These types of class maps have a Class Map Name and a Used By column A sample table for HTTP follows.

Class Map Name	Used By
http-rqst	pmap-5
http-rsp-body	pmap-5

Instant Messaging Service Groups and Peer-to-Peer Application Service Groups

Instant Messaging Service group and peer-to-peer (P2P) application service groups have an additional column because class maps are configured for a specific application, such as the Yahoo! Messenger instant messaging application or the gnutella P2P application. The following table shows sample data for P2P application service groups

Class Map Name	Used By	Class Map Type
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

Details of Class Map

The Details of Class Map area shows the configuration for a particular class map. It has an Item Name and an Item Value column.

Item Name

The name of the configuration setting. For example, an HTTP class map might have settings for Request Header, Port Misuse, and Protocol Violation.

Item Value

The value of the configuration setting. For example, HTTP Request Header seting value might be Length > 500, and the Port Misuse flag might be disabled.

More Information About Class Map Details

For more information about class map details displayed in these windows, click any of the following links:

- Add or Edit a QoS Class Map
- Add or Edit an Inspect Class Map
- Add an HTTP Inspection Class Map
- Add or Edit an Instant Messaging Class Map
- Add or Edit a Point-to-Point Class Map
- Add or Edit an SMTP Class Map

- Add or Edit a SUNRPC Class Map
- Add or Edit an IMAP Class Map
- Add or Edit a POP3 Class Map

Add or Edit an Inspect Class Map

Creating an inspect class map enables you to make a wide variety of traffic available for inspection. Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name. When you have specified the conditions that you want the class to map, click **OK**.

Specifying whether you want the class to match any or all of the conditions

Click **Any** if the class needs to match one or more conditions that you choose. Click **All** if the class must match all the conditions.

Choosing what you want the inspect class map to match

Browse what you want the class map to match in the left column. Click the plus sign (**+**) next to a node to display the child nodes. For example, click **HTTP** to display the child nodes http and https. To choose an item, click it and then click **Add>>**. To remove an item that you have added to the column on the right, click it and then click **<<Remove**.

Changing the match order

If you chose **Any** to match any of the conditions, you may want to change the match order of the items in the right column. To move an item up the list, click it and then click **Up**. To move an item down the list, click it and then click **Down**. The Up button is disabled when you click the item at the top of the list. The Down button is disabled when you click the item at the bottom of the list.

Associate Parameter Map

This dialog displays the parameter maps that you can associate with the class map. Click the **Select** box next to the parameter map you want to associate with the class map.

Add an HTTP Inspection Class Map

HTTP inspection class maps allow you to make a wide variety of HTTP request, response, and request response data available for inspection.

To create an HTTP inspection class map, follow these steps:

Step 1 Enter a class name to identify the class map. You can also enter a description that will be displayed in the HTTP Class Maps window.

Step 2 Click the branch in the HTTP tree that contains the type of data you want to make available for inspection. You can create a class map for HTTP requests, responses, and request-responses.

Step 3 Click the appropriate sub-branch to further specify the type of data you want to include.

Step 4 Configure the class map data in the fields displayed.

Step 5 To specify match conditions, click **Any conditions below** if the class map must match only one or more conditions. Click **All the specified conditions below** if the class map must match all the conditions that you specified.

HTTP Request Header

Enter class map criteria for HTTP request header attributes.

Length Greater Than

Click this box to specify a global request header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of request header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings that you are inspecting for. See Add or Edit Regular Expression for more information about creating regular expressions. To examine an existing map without leaving this dialog, choose the map in the **Select an existing map** list, and click **View**.

Field Name and Configuration Options

You can include fields within the header to the inspection criteria and specify length, count, and strings to inspect for. Click **Add** to include a field, and enter criteria in the dialog displayed.

HTTP Request Header Fields

Choose the type of header field from the list, and specify the inspection criteria for it.

Length Greater Than

Click this box to specify a length that this field should not exceed, and enter the number of bytes. For example, you might block a request whose cookie field exceeds 256 bytes, or whose user-agent field exceeds 128 bytes.

Count Greater Than

Click this box to specify the number of times that this field can be repeated in the header, and enter a number. For example you might block a request that has multiple content-length header lines by entering the value 1. This example is an effective measure for preventing session smuggling.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings that you are inspecting for. See Add or Edit Regular Expression for more

information about creating regular expressions. To examine an existing map without leaving this dialog, choosethe map in the **Select an existing map** list, and click **View**.

Match Field

Check this box to match the class map to the field type that you chose.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the content-type field, you can inspect for content type mismatches between the request and the response, unknown content types, and protocol violations for the particular content type. If you choose the transfer-encoding field, you can inspect for various types of compression and encoding.

HTTP Request Body

You can inspect an HTTP request body for length and character strings.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the length of the request body. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

To inspect for strings, click this box. Choose an existing regular expression class map, or create a new regular expression class map that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

HTTP Request Header Arguments

You can inspect for the length of the arguments sent in a request, and inspect for strings that match regular expressions that you have configured.

Length greater Than

Click this box to specify the number of bytes that the total length of request header arguments should not exceed.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

HTTP Method

HTTP methods indicate the purpose of an HTTP request. Choose the HTTP methods in the Method List column that you want to inspect and check the **Select** box next to the method.

Request Port Misuse

HTTP port #80 is sometimes used by IM, P2P, tunneling, and other applications. Check the types of port misuse that you want to inspect for. You can inspect for any type of port misuse, port misuse by IM applications, P2P application port misuse, and misuse by tunneling applications

Request URI

Enter the Universal Resource Identifier (URI) criteria that you want to include in the class map.

Length Greater Than

Click this box to specify a URI length that a packet should not exceed, and enter the number of bytes.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Sample Use Case

Configure an HTTP class map to block a request whose URI matches any of the following regular expressions:

".*cmd.exe"

".*sex"

".*gambling"

Response Header

Enter the criteria for HTTP response headers that you want to include in the class map.

Length Greater Than

Click this box to specify a global response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more

information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Response Header Fields

Choose the type of header field from the list, and specify the inspection criteria for it.

Length Greater Than

Click this box to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, inspect for unknown content types, and inspect for protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box the class map to match the field type that you chose.

HTTP Response Body

Specify the HTTP response body criteria to inspect for.

Java Applets in HTTP Response

Check this box to inspect for Java applets in the HTTP response.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Response Status Line

Click this box and specify regular expressions to be matched against response status lines. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for.

Sample Use Case

Configure the router to log an alarm whenever an attempt is made to access a forbidden page. A forbidden page usually contains a 403 status-code and the status line looks like "HTTP/1.0 403 page forbidden\r\n."

The regular expression for this is the following:

```
[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403
```

Logging is specified in the policy map to which the HTTP class map is associated.

See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Header Criteria

Enter class map criteria for HTTP request/response headers.

Length Greater Than

Click this box to specify a global request/response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of request/response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Request/Response Header Fields

Choose the HTTP Request/Response header field that you want to include in the class map.

Length Greater Than

Click this box to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, inspect for unknown content types, and inspect for protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box if you want the class map to match the field type that you chose.

Request/Response Body

The router can inspect for request/response body length and specific text strings inside the body of the request/response.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the request/response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Protocol Violation

To inspect for protocol violations in HTTP request/responses, click **Protocol Violation**.

Add or Edit an IMAP Class Map

Creating a class map for Internet Message Access Protocol (IMAP) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect IMAP traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect IMAP traffic for invalid commands.

Add or Edit an SMTP Class Map

Simple Mail Transfer Protocol (SMTP) class maps enable you to limit content length and enforce protocol compliance.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description in the field provided.

In the **Maximum data transfer allowed in a session** field, enter the maximum number of bytes the router should allow for an SMTP session.

Add or Edit a SUNRPC Class Map

SUN Remote Procedure Call (SUNRPC) class maps allow you to specify the number of the program whose traffic you want the router to inspect.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Add** in the **Match Program Number** box to add a program number.

Add or Edit an Instant Messaging Class Map

Instant Messaging (IM) class maps allow you to specify the type of instant messaging and whether you want traffic for all IM services inspected, or only traffic for the text chat service.

In the **Class Map Type** field, choose **aol** for America Online, **msnmsgr** for Microsoft Networks Messenger, or choose **ymsgr** for Yahoo! Messenger.

In the Match Criteria box, click **All services**, or click **Text chat services** if you want only text chat traffic to be inspected.

Add or Edit a Point-to-Point Class Map

A P2P class map specifies a P2P application and the match criteria. Only one application can be specified per class map.

Class Name

Enter a new class name to create a new class map. Clicking the button at the right of the field allows you to select existing class maps to edit. You can edit the match criteria for a class map, but you cannot change the class map type.

Class Map Type

You can create a P2P class map for the following types of P2P services:

- eDonkey
- fasttrack
- gnutella
- kazaa2

Match Criteria and Value

Click **Add** to enter match criteria to specify the type of connections to be identified by the traffic class.

Enter match criteria to specify the type of connections that are to be identified by the traffic class. You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search file name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter *****.

Add P2P Rule

Enter match criteria to specify the type of connections that are to be identified by the traffic class. You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search-file-name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter *****.

Add or Edit a POP3 Class Map

Creating a class map for Post Office Protocol version 3 (POP3) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect POP3 traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect POP3 traffic for invalid commands.

Parameter Maps

Parameter Maps specify inspection behavior for Zone-Policy Firewall, for parameters such as denial-of-service protection, session and connection timers, and logging settings, Parameter Maps are also applied with Layer 7 class maps and policy maps to define application-specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application-specific information.

Parameter Map Windows

The parameter map windows list the configured parameter maps for protocol information, URL filtering, regular expressions, and other types of parameter maps. If a parameter map has been associated with a class map, the class map name appears in the Used By column. The details of the selected parameter map are displayed in the bottom half of the window. You can add, edit, and delete parameter maps. Cisco SDM informs you if you attempt to delete a parameter map that is being used by a class map.

For more information about the parameter maps displayed in these windows, click any of the following links:

- Timeouts and Thresholds for Inspect Parameter Maps and CBAC
- Add or Edit a Parameter Map for Protocol Information
- General Settings for URL Filtering
- Add or Edit a URL Filter Server
- Local URL List
- Add or Edit Regular Expression

Add or Edit a Parameter Map for Protocol Information

It may be necessary to identify servers for specific types of applications, such as IM applications so that you can restrict use to a particular activity, such as text chat.

Parameter Map Name

Enter a name that conveys the use of this parameter map. For example, if you are creating a server list for Yahoo! Instant Messenger text chat servers, you can enter the name **ymsgr-pmap**.

Server Details

This area of the screen is a list of server names, server IP addresses, or IP address ranges.

Add or Edit a Server Entry

You can provide the hostname or IP address of an individual server, or a range of IP addresses assigned to a group of servers.

You can enter a hostname in the **Name** field if the router is able to contact a DNS server on the network to resolve the server's IP address. To enter the IP address for one server, enter it in the **Single IP Address** field. If there are several servers that use an IP address range, use the **IP range** field. Enter the lowest IP address in the left-hand field and the highest IP address in the right hand field. For example to enter the range 103.24.5.67 through 99, enter **103.24.5.67** in the left-hand field and **103.24.5.99** in the right-hand field.

Add or Edit Regular Expression

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

The regular expressions that you create can be used anywhere in which a regular expression is needed in the Zone-Based Policy Firewall screens. Regular Expression Metacharacters lists regular expression metacharacters and how they are used.

Name

Enter a name to identify the regular expression. If you are editing the regular expression, the name field is read only.

Pattern List

A regular expression can contain multiple patterns. Click **Add** to display a dialog in which you can enter a new regular expression pattern. Each pattern that you create is automatically added to the list. If you need to copy a pattern from another regular expression, click **Copy Pattern**, click the plus (**+**) sign next to regular expression name, click the pattern that you want, and then click **OK**.

Here is an example pattern list.

```
parameter-map type regex ref_regex
pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"
parameter-map type regex host_regex
pattern "secure\.keenvalue\.com"
pattern "\.looksmart\.com"
parameter-map type regex usragnt_regex
pattern "Peer Points Manager"
```

Add a Pattern

The pattern that you enter in this window is added at the bottom of the regular expression parameter map that you are editing. If you need to reorder the patterns in the parameter map, you can do so in the Edit Regular Expression window.

Pattern

Enter the pattern that you want to add to the regular expression.

Guide Button

Click the **Guide** Button to display the Build Regular Expression dialog, which can assist you in constructing a regular expression. If you click **Guide**, any text that you entered in the **Pattern** field appears in the Regular Expression field of the Build Regular Expression dialog.

Build Regular Expression

The Build Regular Expression dialog box lets you construct a regular expression from characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.

Build Snippet

This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- Starts at the beginning of the line (^)—To indicate that the snippet should start at the beginning of a line, use the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.

- Specify Character String—Enter a text string manually.

    - Character String—Enter a text string.

    - Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. For example, if you enter "example.com," this option converts it to "example\.com".

    - Ignore Case—To match uppercase and lowercase characters, this check box automatically adds text to match both uppercase and lowercase characters. For example, "cats" converts to "[cC][aA][tT][sS]".

Specify Character

This area lets you specify a metacharacter to insert in the regular expression.

- Negate the character—Specifies not to match the character you identify.

- Any character (.)—Inserts the period (.) metacharacter to match any character. For example, "d.g" matches *dog*, *dag*, *dtg*, and any word that contains those characters, such as *doghouse*.

- Character set—Inserts a character set. Text can match any character in the set. Sets include:

    [0-9A-Za-z]

    [0-9]

    [A-Z]

[a-z]

[aeiou]

[\n\f\r\t] (which matches a new line, form feed, return, or a tab)

For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (uppercase or lowercase) or any digit 0 through 9.

- Special character—Inserts a character that requires an escape, including \, ?, *, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.

- Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).

- Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.

- Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.

- Specified character—Enter any single character.

Snippet Preview

Display only. Shows the snippet as it will be entered in the regular expression.

- Append Snippet—Adds the snippet to the end of the regular expression.

- Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.

- Insert Snippet at Cursor—Inserts the snippet at the cursor.

Regular Expression

This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- Selection Occurrences—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is "test me," and you select "me" and apply **One or more times**, then the regular expression changes to "test (me)+".

- Zero or one times (?)—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.

- One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.

- One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.

- Any number of times (*)—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.

- At least—Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.

- Exactly—Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.

- Apply to Selection—Applies the quantifier to the selection.

Regular Expression Metacharacters

The following table lists the metacharacters that have special meanings.

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp*)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.

Character	Description	Notes
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x*}	Repeat quantifier	Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
{*x*,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
[*abc*]	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc*]	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a*-*c*]	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does **[a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **" test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, \[matches the left square bracket.

Character	Description	Notes
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

URL Filtering

URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in a URL list. You can maintain a local URL list on the router, and you can use URL lists stored on Websense or Secure Computing URL filter list servers. URL filtering is enabled by configuring an Application Security policy that enables it.

Even if no Application Security policy is configured on the router, you can still maintain a local URL list and a URL filter server list that can be used for URL filtering when a policy is created that enables it.

This chapter contains the following sections:

- URL Filtering Window
- Local URL List
- URL Filter Servers

For more information on URL filtering, go to the following link:

Firewall Websense URL Filtering

To learn how URL filtering policies are used, click URL Filtering Precedence.

URL Filtering Window

This window displays the global settings for URL filtering on the router. You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The Global settings for URL filtering can only be maintained from this Additional Tasks window. Use the **Edit Global Settings** button to change these values.

For a description of each setting that appears in this window, Click Edit Global Settings.

See the introductory information in URL Filtering for a description of the URL filtering features that Cisco SDM provides.

Edit Global Settings

Edit URL filtering global settings in this window.

> **Note** Logging must be enabled for the router to report URL filter alerts, audit trail messages, and system messages pertaining to the URL filter server.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.

Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.

Maximum buffered HTTP requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum buffered HTTP responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

General Settings for URL Filtering

Name the URL filter, specify what the router is to do when it detects a match, and configure log and cache size parameters. You can also specify a source interface if you do not want the URL filtering parameter map to apply to all router interfaces.

URL Filter Name

Enter a name that will convey how this URL filter is configured or used. For example, if you specify a source interface of Fast Ethernet 1, you might enter the name **fa1-parmap**. If the filter uses a Websense URL filter server at IP address 192.128.54.23, you might enter **websense23-parmap** as the name.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.

Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.

Maximum Buffered HTTP Requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum Buffered HTTP Responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

Advanced

The Advanced box allows you to choose the source interface. Choose the interface from the Source Interface list.

Local URL List

If the Cisco IOS image on the router supports URL filtering but does not support Zone-based Policy Firewall (ZPF), you can maintain one local URL list on the router. This list is used by all Application Security policies in which URL filtering is enabled. Cisco IOS images of release 12.4(9)T and later support all the ZPF features that SDM supports. In a ZPF configuration, a local URL list can be created for each URL filtering parameter map.

You can use Cisco SDM to create list entries and you can import entries from a list stored on your PC. When a local URL list is used in combination with URL filter servers, local entries are used first. See URL Filtering Precedence for more information.

Maintaining the Local URL List

You can use Cisco SDM to maintain a local URL list by adding and deleting entries one-by-one, and by importing a URL list from your PC and specifying what you want Cisco SDM to do with each entry. Use the **Add** and the **Delete** buttons to manage specific entries in the list on the router, and click the **Import URL List** button to import a URL list from your PC.

Note If an entry is deleted from the local list and the router is configured to use URL filtering servers, entries that match ones that you are deleting from the local list may exist on those servers.

Use the **Delete All** button to delete all entries on the router. If no local list is configured on the router, the router must rely on the configured URL filter servers. If you want to retrieve the URL list you are deleting at a later time, use the **Export URL List** button to save the URL list to your PC before deleting all the entries. When you save a URL list to your PC the list is given a .CSV extension.

Importing URL Lists from your PC

Click the **Import URL List** button to import a URL list from your PC to the router. The URL list that you select must have a .txt or .CSV extension. After you select the list on your PC, Cisco SDM displays a dialog that allows you to specify what you want to do with each entry in the list. See Import URL List for more information.

Add or Edit Local URL

Use this window to add or edit a URL entry for the local URL list on the router. Enter a full domain name or a partial domain name and choose whether to **Permit** or **Deny** requests for this URL.

If you enter a full domain name, such as www.somedomain.com, all requests that include that domain name, such as www.somedomain.com/news or www.somedomain.com/index will be permitted or denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.

If you enter a partial domain name, such as .somedomain.com, all requests that end with that string, such as www.somedomain.com/products or wwwin/somedomain.com/eng will be permitted denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.

Import URL List

This dialog allows you to examine the URL list you are importing from your PC to the router and specify what you want to do with each entry. If a URL entry in this dialog is not already present on the router, you can add it to the list on the router by clicking **Append**. If a URL entry is already present on the router but you want to replace it with the entry in this dialog, click **Replace**.

All boxes in the **Import** column are checked by default. If there are entries that you do not want to be sent to the router, uncheck the box next to those entries. If you want to remove the checks from all the boxes, click **Unselect All**. Clicking **Select All** places checkmarks in all the boxes.

Append adds any checked entry to the URL list that is not already present in the list If you attempt to add an entry that is already in the URL list, it will not be added even if the action specified for the domain in the entry is different from the action that is already in the list.

Use the **Replace** button to specify a different action for an entry that is already in the router's URL list. If the entry you checked is not already in the router's list, **Replace** has no effect.

URL Filter Servers

The router can send HTTP requests to URL filtering servers that are capable of storing much larger URL lists than the router can store. If the router is configured with a URL filter server list, the router sends requests that do not match entries in the local list to the URL filter server it has a connection to, and permits or denies the request based on the response it receives from the server. When the server that the router is connected to goes down, the router contacts the next server in the list until it establishes a connection.

Lists on URL filter servers can be used along with local URL lists. Click URL Filtering Precedence to learn how the router uses both of these resources.

Click **Add**, and choose either **Secure Computing** or **Websense** to specify the type of server that you are adding.

✎

Note   Cisco IOS software can only use one type of URL filtering server, and does not allow you to add a server to the list if it is of a different type. For example, if a URL filter server list containing Websense servers is configured on the router, you

will receive an error message if you attempt to add an Secure Computing server to the list. If the URL filter server list currently contains one type of server and you want to change to the other type, you must delete all the server entries in the list before adding an entry of the new type.

This window displays the configuration for each URL filter server in the list. See Add or Edit a URL Filter Server for a description of each configuration value.

Add or Edit a URL Filter Server

Specify the information for the Websense or Secure Computing URL filter server.

IP Address/Hostname

Enter the IP address or the hostname for the server. If you enter a hostname, the router must have a connection to a DNS server in order to resolve the hostname to an IP address.

Direction

Choose **Inside** if the URL filter server is part of the inside network. This is usually one of the networks that the router LAN interfaces connect to. Choose **Outside** if the router is in the outside network. This is usually one of the networks that the router WAN interfaces connect to. The default value is **Inside**.

Port Number

Automatically contains the default port number for the type of URL filter server you are adding. If you are adding a Websense server, the default value is 15868. If you are adding an Secure Computing server, the default value is 4005. Change this number to the number of the port that the server listens on if that number is different from the default. This field accepts values from 1 to 65535.

Retransmission Count

Optional field. Enter the number of times that you want the router to attempt to retransmit the request if no response arrives from the server. The default value is 2 times. This field accepts values from 1 to 10.

Retransmission Timeout

Optional field. Enter the number of seconds that the router should wait for a response from the server before retransmitting the request. The default value is 5 seconds.

URL Filtering Precedence

URL filtering must be enabled by going to **Configure > Firewall and ACL > Application Security > URL Filtering** and clicking **Enable URL filtering**. This can only be done when an Application security policy is configured on the router.

When URL filtering is enabled, the router determines how to handle an HTTP request as follows:

- If the URL in the request matches an entry in the local URL list on the router, the router permits or denies the request based on that entry.

- If the URL in the request does not match any entry in the local URL list, the router passes the HTTP request to the URL filtering server to which it has a connection. It permits or denies the request based on the information that the server returns.

- If allow mode is disabled, and the router cannot establish a connection with a URL filter server, the router denies the request. Allow mode is disabled by default.

- If allow mode is enabled and the router cannot establish a connection with a URL filter server, the router permits the request. Allow mode can be enabled in the Edit Global Settings dialog.

Only one URL list and one URL filter server list can be configured on the router. All configured Application Security policies use the same URL list and URL filter server list. These lists can be maintained in the Application Security windows, or by going to **Additional Tasks > URL Filtering**. If all Application Security policies are deleted, the URL list and URL filter server list can still be maintained in the Additional Tasks windows. However, the router does not perform URL filtering unless URL filtering is enabled in an Application Security policy.

Configuration Management

Cisco SDM allows you to edit the router configuration file and to reset the router configuration to factory defaults. Because editing the configuration file directly and resetting the router to factory defaults can cause you to lose the connection between the PC and the router, be sure to read the online help for all screens in this area of Cisco SDM.

Manually Editing the Configuration File

Cisco SDM allows you to edit the router configuration file by providing a configuration editor that you can use to import a configuration file or use to enter Cisco IOS CLI commands directly.

Cisco SDM supports the most widely-used Cisco IOS commands and keywords, but it cannot support every CLI command. If you are experienced with the Cisco IOS CLI and have an excellent understanding of how the configuration commands that you want to enter will affect the behavior of the router and the network in which it resides, you may find that using the configuration editor is faster than using Cisco SDM dialogs. If you want to add a configuration that Cisco SDM does not support, you must either use the Config Editor to do so, or open a Telnet session with the router and use the Cisco IOS CLI.

Using the Config Editor bypasses Cisco SDM validation. Although Cisco SDM returns IOS error messages, it cannot compare your configuration changes against the running configuration and inform you of conflicts thay may result. For example, if you use Cisco SDM dialogs to enter a VPN configuration on a router that already has a firewall configuration, Cisco SDM examines the firewall and determines which permit statements must be added to enable VPN traffic to pass

through, and is able to make them for you. However, if you use the Config Editor, you must determine which conflicts may result by examining the existing configuration and making any additional changes needed to resolve those conflicts, and then monitor router behavior to see if it handles traffic as you intend it to.

Although it is not required, it is strongly recommended that you allow Cisco SDM to back up the current running configuration. When Cisco SDM performs this backup, it uses the same filename each time, thus overwriting any earlier backup file.

Config Editor

The Config Editor lets you view the running configuration and make changes to it by editing specific commands or by replacing the entire configuration file with one that you import from your PC. You can view the running configuration as you make changes, or you can use the entire window to view the configuration that you are sending to the router.

Running Configuration

By default, this box displays the router running configuration. You can hide this box by clicking **Hide** in the upper-right-hand corner of the window. Redisplay this box by clicking **Show**.

Edit Configuration

Perform edits in this box. By default, this box is empty. Fill it with the router running configuration by clicking **Import** > **running config**. Fill it with a configuration file on the PC by clicking **Import** > **config from PC**. Increase the size of this box by hiding the Running Configuration box.

Merging with Running Config

If you want to merge changes that you have made in the Edit Configuration box with the router running config, click **Merge with Running Config**. The changes are sent to the router and take effect as soon as the router receives them.

Replacing the Running Config

If you want to replace the running config with the contents of the Edit Configuration box, click **Replace Running Config**. You should not use this button unless you have populated the Edit Configuration box with a configuration that you have imported from the router and edited, or a configuration that you have imported from your PC.

Restore

If you saved the running configuration before using the Config Editor, you can restore that configuration to your router by clicking this button. The restored configuration is copied to the router's startup configuration, and the router is reloaded. If no backup copy of the router's configuration exists, Cisco SDM displays a message informing you that it cannot restore the configuration.

Reset to Factory Defaults

You can reset the configuration of the router to factory defaults and save the current configuration to a file that can be used later. If you changed the router's LAN IP address from the factory value 10.10.10.1, you will lose the connection between the router and the PC because that IP address will change back to 10.10.10.1 when you reset.

Note
- The Reset to Factory Defaults feature is not supported on Cisco 3620, 3640, 3640A, and 7000 series routers.

- The Reset to Factory Defaults feature is not supported when you are running a copy of Cisco SDM installed on the PC.

Before you start, you should understand how to give your PC a static IP address in the 10.10.10.0 subnet so that you will be able to reconnect to the router after you reset it. The factory configuration does not include a DHCP server configuration on the router, and the router will not give an IP address to the PC. In addition, the factory configuration limits HTTP or HTTPS access to the router,

restricting it to the LAN interface, and only from the internal subnet defined on that interface. After you access the router, you can change the router default IP address and set it to allow remote access.

Understanding How to Give the PC a Dynamic or Static IP Address After You Reset

If you want to use Cisco SDM after you reset, you have to give your PC a static or dynamic IP address, depending on the type of router that you have. Use the following table to determine the type of address to give the PC.

Routers Needing Dynamic Addresses	Routers Needing Static Addresses
SB10x	Cisco 1721, 1751, and 1760
Cisco 83x, 85x, and 87x	Cisco 1841
Cisco 1701, 1710, and 171x	Cisco 2600XM, and 2691
Cisco 180x and 181x	Cisco 28xx, 36xx, 37xx, and 38xx

The process for giving the PC a static or dynamic IP address varies slightly depending on the version of Microsoft Windows the PC is running.

Note   Do not reconfigure the PC until after you reset the router.

Microsoft Windows NT

From the Control Panel, double-click the **Network** icon to display the Network window. Click **Protocols**, select the first TCP/IP Protocol entry, and click **Properties**. In the Properties window, select the Ethernet adapter used for this connection. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address. For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. Click **OK**.

Microsoft Windows 98 and Microsoft Windows ME

From the Control Panel, double-click the **Network** icon to display the Network window. Double-click the TCP/IP Protocol entry with the Ethernet adapter being used for this connection to display TCP/IP **Properties**. In the IP address tab, click **Obtain an IP Address Automatically** to obtain a dynamic IP address. For a static

IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. Click **OK**.

Microsoft Windows 2000

From the Control Panel, select **Network and Dialup Connections/Local Area Connections**. Select the Ethernet adapter in the Connect Using field. Select Internet Protocol, and click Properties. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address. For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. Click **OK**.

Microsoft Windows XP

Click **Start**, select **Settings**, **Network Connections**, and then select the LAN connection you will use. Click **Properties**, select **Internet Protocol TCP/IP**, and click the **Properties** button. Click **Obtain an IP Address Automatically** to obtain a dynamic IP address. For a static IP address, click **Specify an IP address**. Enter the IP address 10.10.10.2 or any other address in the 10.10.10.0 subnet greater than 10.10.10.1. Enter the subnet 255.255.255.248. Click **OK**.

To Reset the Router to Factory Defaults:

Step 1   Leave **Save Running Config to PC** checked in **Step 1** on screen, and specify a name for the configuration file. Cisco SDM provides a default path and name. You don't have to change it unless you want to.

Step 2   Review the information in the Understand How to Reconnect box in **Step 2** on screen so that you will be able to establish a connection to the router after you reset. If necessary, review the information in **Understanding How to Give the PC a Dynamic or Static IP Address After You Reset.**

Step 3   Click **Reset Router**.

Step 4   Click **Yes** to confirm the reset.

Step 5   Follow the procedure in the' Understand How to Reconnect box in **Step 2** to reconnect.

Resetting the router to its factory default configuration changes the router's inside interface IP address back to 10.10.10.1. The next time you log on to the router with your browser, enter the IP address 10.10.10.1 in the browser's location field.

This Feature Not Supported

This window appears when an Cisco SDM feature is not supported. This may be because the router is running a Cisco IOS image that does not support the feature, or because Cisco SDM is being run on a PC and cannot support the feature.

C H A P T E R **40**

More About....

These topics provide more information about subjects that Cisco SDM online help discusses.

IP Addresses and Subnet Masks

This topic provides background information about IP addresses and subnet masks, and shows you how to use this information when entering addresses and masks in Cisco SDM.

IP version 4 addresses are 32 bits, or 4 bytes, in length. This address "space" is used to designate the following:

- Network number
- Optional subnetwork number
- A host number

> **Note** Cisco SDM does not support IP version 6.

Cisco SDM requires you to enter IP addresses in dotted-decimal format. This format makes addresses easier for people to read and manipulate, by grouping the 32 bits into 4 octets which are displayed in decimal, separated by periods or "dots," for example, 172.16.122.204. The decimal address 172.16.122.204 represents the binary IP address shown in the following figure.

Decimal   172 . 16 . 122 . 204
Binary   10101100 00010000 01111010 11001100

The subnet mask is used to specify how many of the 32 bits are used for the network number and, if subnetting is used, the subnet number. It is a binary mask with a 1 bit in every position used by the network and subnet numbers. Like the IP address, it is a 32-bit value, expressed in decimal format. The following figure shows a subnet mask entered in Cisco SDM. Cisco SDM shows the subnet mask and the equivalent number of bits in the mask.

Subnet Mask: 255.255.255.0   or   24

These values entered Cisco SDM represent the binary mask shown in the following figure:

Decimal   255 . 255 . 255 . 0
Binary   11111111 11111111 11111111 00000000
                    24 bits

This subnet mask specifies that the first 24 bits of the IP address represent the network number and subnet mask, and that the last 8 bits represent the host number within that network and subnet. You can enter the mask in the dotted decimal format shown in the Subnet Mask field, or you can select the number of bits in the bits field. When you enter or select a value in one field, Cisco SDM automatically adjusts the other.

Cisco SDM displays a warning window if you enter a decimal mask that results in binary zeros (0s) in the network/subnet area of the mask. The following subnet mask field contains a decimal value that would result in binary zeros in the network/subnet number portion of the mask. Note that the bits field on the right is empty, indicating that an invalid value has been entered in the Subnet Mask field.
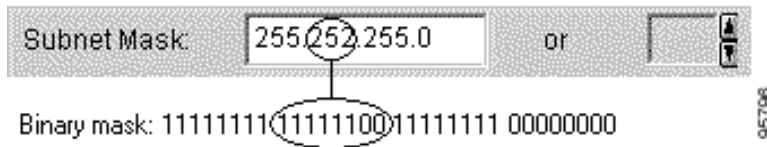
When a network address is displayed in Cisco SDM windows, the IP address and subnet mask for it may be shown in network address/subnet bits format, as in the following example:

```
172.28.33.0/24
```

The network address in this example is 172.28.33.0. The number 24 indicates the number of subnet bits used. You can think of it as shorthand for the corresponding subnet mask of 255.255.255.0.

Addresses used on the public Internet must be completely unique for the period of time they are being used. On private networks, addresses may be unique only to the private network or subnetwork.

Addresses may also be translated by using schemes such as NAT and PAT, and they may be temporarily assigned using DHCP. You can use Cisco SDM to configure NAT, PAT and DHCP.

Host and Network Fields

This topic explains how to supply host or network information in windows that allow you to specify a network or host address, or a host name.

Specify the network or the host.

Type

One of the following:

- **A Network**—If you select this, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.

- **A Host Name or IP Address**—If you select this, provide a host IP address or host name in the next field.

- **Any IP address**—The action you specified is to apply to any host or network.

IP Address/Wildcard Mask

Enter a network address, and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you selected **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network capable of resolving the host name to an IP address.

Available Interface Configurations

The types of configurations available for each interface type are shown in the following table.

If you have selected:	You can add a:
An Ethernet interface	• PPPoE connection • Tunnel interface • Loopback interface
Any of the following: • Ethernet with a PPPoE connection • Dialer Interface associated with an ADSL or G.SHDSL configuration • Serial interface with a PPP or HDLC configuration • Serial subinterface with a Frame Relay configuration • Unsupported WAN interface	• Tunnel interface • Loopback Interface

An ATM interface without any encapsulation	• An ADSL interface
	• A G.SHDSL interface
	• A tunnel or loopback for either of the above
A serial interface	• A Frame Relay connection
	• A PPP connection
	• A tunnel interface
	• A loopback interface
ATM subinterface An Ethernet subinterface A dialer interface not associated with an ATM interface A loopback A tunnel	• A tunnel interface • A loopback interface

DHCP Address Pools

The IP addresses that the DHCP server assigns are drawn from a common pool that you configure by specifying the starting IP address in the range and the ending address in the range.

The address range that you specify should be within the following private address ranges:

- 10.1.1.1 to 10.255.255.255
- 172.16.1.1 to 172.31.255.255

The address range that you specify must also be in the same subnet as the IP address of the LAN interface. The range can represent a maximum of 254 addresses. The following examples are valid ranges:

- 10.1.1.1 to 10.1.1.254 (assuming LAN IP address is in 10.1.1.0 subnet)
- 172.16.1.1 to 172.16.1.254 (assuming LAN IP address is in 172.16.1.0 subnet)

Cisco SDM configures the router to automatically exclude the LAN interface IP address in the pool.

Reserved Addresses

You must not use the following addresses in the range of addresses that you specify:

- The network/subnetwork IP address.

- The broadcast address on the network.

Meanings of the Permit and Deny Keywords

Rule entries can be used in access rules, NAT rules, IPSec rules, and in access rules associated with route maps. Permit and Deny have various meanings depending on which type of rule is using it.

Rule Type	Meaning of Permit	Meaning of Deny
Access rule	Allow matching traffic in or out of the interface to which the rule has been applied.	Drop matching traffic.
NAT rule	Translate the IP address of matching traffic to the specified inside local address or outside local address.	Do not translate the address.
IPSec rule (Extended only)	Encrypt traffic with matching address.	Do not encrypt traffic. Allow it to be sent unencrypted.
Access rule used in route map	Protect matching addresses from NAT translation.	Do not protect matching addresses from NAT translation.

Services and Ports

This topic lists services you can specify in rules, and their corresponding port numbers. It also provides a short description of each service.

This topic is divided into the following areas:

- TCP Services

- UDP Services

- ICMP Message Types

- IP Services
- Services That Can Be Specified in Inspection Rules

TCP Services

TCP Service	Port Number	Description
bgp	179	Border Gateway Protocol.BGP exchanges reachability information with other systems that use the BGP protocol
chargen	19	Character generator.
cmd	514	Remote commands. Similar to exec except that cmd has automatic authentication
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name Service. System used on the Internet for translating names of etwork nodes into addresses.
echo	7	Echo request. Message sent when ping command is issued.
exec	512	Remote process execution
finger	79	Finger. Application that determines whether a person has an account at a particular internet site.
ftp	21	File Transfer Protocol. Application-layer protocol used for transferring files between network nodes.
ftp-data	20	FTP data connections
gopher	70	Gopher. A distributed document delivery system.
hostname	101	NIC hostname server
ident	113	Ident Protocol
irc	194	Internet Relay Chat. A world-wide protocol that allows users to exchange text messages with each other in real time.
klogin	543	Kerberos login. Kerberos is a developing standard for authenticating network users.
kshell	544	Kerberos shell
login	513	Login

TCP Service	Port Number	Description
lpd	515	Line Printer Daemon. A protocol used to send print jobs between UNIX systems.
nntp	119	Network News Transport Protocol.
pim-auto-rp	496	Protocol-Independent Multicast Auto-RP. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.
pop2	109	Post Office Protocol v2. Protocol that client e-mail applications use to retrieve mail from mail servers.
pop3	110	Post Office Protocol v3
smtp	25	Simple Mail Transport Protocol. Internet protocol providing e-mail services.
sunrpc	111	SUN Remote Procedure Call. See rpc.
syslog	514	System log.

UDP Services

UDP Service	Port Number	Description
biff	512	Used by mail system to notify users that new mail is received
bootpc	69	Bootstrap Protocol (BOOTP) client
bootps	67	Bootstrap Protocol (BOOTP) server
discard	9	Discard
dnsix	195	DNSIX security protocol auditing
domain	53	Domain Name Service (DNS)
echo	7	See echo.
isakmp	500	Internet Security Association and Key Management Protocol
mobile-ip	434	Mobile IP registration
nameserver	42	IEN116 name service (obsolete)
netbios-dgm	138	NetBios datagram service. Network Basic Input Output System. An API used by applications to request services from lower-level network processes.

UDP Service	Port Number	Description
netbios-ns	137	NetBios name service
netbios-ss	139	NetBios session service
ntp	123	Network Time Protocol. TCP protocol that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet.
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
rip	520	Routing Information Protocol. A protocol used to exchange route information between routers.
snmp	161	Simple Network Management Protocol. A protocol used to monitor and control network devices.
snmptrap	162	SNMP trap. A system management notification of some event that occurred on the remotely managed system.
sunrpc	111	SUN Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client.
syslog	514	System log service.
tacacs	49	Terminal Access Controller Access Control System. Authentication protocol that provides remote access authentication and related services, such as logging.
talk	517	Talk. A protocol originally intended for communication between teletype terminals, but now a rendezvous port from which a TCP connection can be established.
tftp	69	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred between network nodes.
time	37	Time.
who	513	Port to databases showing who is logged in to machines on a local net and the load average of the machine
xdmcp	177	X-Display Manager Client Protocol. A protocol used for communications between X-Displays (clients) and X Display Managers.
non500-isakmp	4500	Internet Security Association and Key Management Protocol. This keyword is used when NAT-traversal port floating is required.

ICMP Message Types

ICMP Messages	Port Number	Description
alternate-address	6	Alternate host address.
conversion-error	31	Sent to report a datagram conversion error.
echo	8	Type of message sent when ping command is issued.
echo-reply	0	Response to an echo-request (ping) message.
information-reply	16	Obsolete. Response to message sent by host to discover number of the network it is on. Replaced by DHCP.
information-request	15	Obsolete. Message sent by host to discover number of the network it is on. Replaced by DHCP.
mask-reply	18	Response to message sent by host to discover network mask for the network it is on.
mask-request	17	Obsolete. Message sent by host to discover network mask for the network it is on.
mobile-redirect	32	Mobile host redirect. Sent to inform a mobile host of a better first-hop node on the path to a destination.
parameter-problem	12	Message generated in response to packet with problem in its header.
redirect	5	Sent to inform a host of a better first-hop node on the path to a destination.
router-advertisement	9	Sent out periodically, or in response to a router solicitation.
router-solicitation	10	Messages sent in order to prompt routers to generate router advertisements messages quickly.
source-quench	4	Sent when insufficient buffer space is available to queue packets for transmission to next hop, or by destination router when packets are arriving too quickly to be processed.
time-exceeded	11	Sent to indicate received packet's time to live field has reached zero.
timestamp-reply	14	Reply to request for timestamp to be used for synchronization between two devices.

ICMP Messages	Port Number	Description
timestamp-request	13	Request for timestamp to be used for synchronization between two devices.
traceroute	30	Message sent in reply to a host that has issued a traceroute request.
unreachable	3	Destination unreachable. Packet cannot be delivered for reasons other than congestion.

IP Services

IP Services	Port Number	Description
aahp	51	
eigrp	88	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco.
esp	50	Extended Services Processor.
icmp	1	Internet Control Message Protocol. Network layer protocol that reports errors and provides other information relevant to IP packet processing.
igmp	2	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to adjacent multicast routers.
ip	0	Internet Protocol. Network layer protocol offering connectionless internetwork service.
ipinip	4	IP-in-IP encapsulation.
nos	94	network operating system. A distributed file system protocol.
ospf	89	Open Shortest Path First. A link-state hierarchical routing algorithm.
pcp	108	Payload Compression Protocol
pim	103	Protocol-Independent Multicast. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.

IP Services	Port Number	Description
tcp	6	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
udp	17	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack.

Services That Can Be Specified in Inspection Rules

Protocol	Description
cuseeme	Videoconferencing protocol.
fragment	Specifies that the rule perform fragment inspection.
ftp	See ftp.
h323	See H.323.
http	See HTTP.
icmp	See icmp.
netshow	NetShow. A streaming video protocol.
rcmd	Remote Comman d. A protocol used when commands are executed on a remote system by a local system.
realaudio	RealAudio. A streaming audio protocol.
rpc	Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client
rtsp	Real-Time Streaming Protocol. An application-level protocol used to control delivery of data with real-time properties.
sip	Session Initiation Protocol. Sip is a telephony protocol used to integrate telephony services and data services.
skinny	A telephony protocol enabling telephony clients to be H.323 compliant.
smtp	See smtp.
sqlnet	Protocol for network enabled databases.
streamworks	StreamWorks protocol. Streaming video protocol.

Protocol	Description
tcp	See tcp.
tftp	See tftp.
udp	See udp.
vdolive	VDOLive protocol. A streaming video protocol.

More About NAT

This section provides scenario information that may help you in completing the NAT Translation Rule windows, and other information that explains why NAT rules created using the CLI may not be editable in Cisco SDM.

Static Address Translation Scenarios

The following scenarios show you how you can use the static address translation rules.

Scenario 1

You need to map an IP address for a single host to a public address. The address of the host is 10.12.12.3. The public address is 172.17.4.8.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from Interface Fields		Translate to Interface Fields	
Static/Dynamic	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	172.17.4.8	Leave unchecked.

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. If this is the only NAT rule for this network, 10.12.12.3 is the only address on the network that gets translated.

Scenario 2

You need to map each IP address in a network to a unique public IP address, and you do not want to create a separate rule for each mapping. The source network number is 10.l2.12.0, and the target network is 172.17.4.0. However, in this scenario, it is not necessary to know the source or target network numbers. It is sufficient to enter host addresses and a network mask.

The following table shows how the fields in the Add Address Translation Rule window would be used.

Static/Dynamic	Translate from Interface Fields		Translate to Interface Fields	
	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.35 (host)	255.255.255.0	172.17.4.8 (host)	Leave unchecked.

Result

NAT derives the "Translate from" network address from the host IP address and the subnet mask. NAT derives the "Translate to" network address from the the net mask entered in the "Translate from" fields, and the "Translate to" IP address. The source IP address in any packet leaving the original network is translated to an address in the 172.17.4.0 network.

Scenario 3

You want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host.

The following table shows how the fields in the Add Address Translation Rule window would be used.

Static/Dynamic	Translate from... fields		Translate to... fields	
	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	172.17.4.8	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 is routed to port number 137 of the host with the IP address 10.12.12.3.

You need to create a separate entry for each host/port mapping that you want to create. You can use the same "Translated to" IP address in each entry, but you must enter a different "Translated from" IP address in each entry, and a different set of port numbers.

Scenario 4

You want source-"Translate from"-addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. You also want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host. The following table shows how the fields in the Add Address Translation Rule window would be used:

	Translate from... fields		Translate to... fields	
Static/Dynamic	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	FastEthernet 0/1	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 & port 139 is routed to port number 137 of the host with the IP address 10.12.12.3.

Dynamic Address Translation Scenarios

The following scenarios show you how you can use dynamic address translation rules. These scenarios are applicable whether you select from inside-to-outside, or from outside-to-inside.

Scenario 1

You want source–"Translate from"–addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. Port Address Translation (PAT) would be used to distinguish traffic associated with different hosts. The ACL rule you use to define the "Translate from" addresses is configured as shown below:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

When used in a NAT rule this access rule would allow any host in the 10.10.10.0 network, except the one with the address 10.10.10.1 to receive address translation.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from... fields	Translate to... fields		
Static/Dynamic	ACL Rule	Type	Interface	Address Pool
Dynamic	7	Interface	FastEthernet0/1	Disabled

Result

Traffic from all hosts on the 10.10.10.0 network would have the source IP address translated to 172.17.4.8. PAT would be used to distinguish traffic associated with different hosts.

Scenario 2

You want the host addresses specified in access-list 7 in the previous scenario to use addresses from a pool you define. If the addresses in the pool become depleted, you want the router to use PAT to satisfy additional requests for addresses from the pool.

The following table shows how the fields in the Address Pool window would be used for this scenario.

Pool Name	Port Address Translation	IP Address fields		Network Mask
Pool 1	Checked	172.16.131.2	172.16.131.10	255.255.255.0

The following table shows how the fields in the Add Address Translation Rule window would be used for this scenario.

| Static/Dynamic | Translate from... fields | Translate to... fields | | |
	ACL Rule	Type	Interface	Address Pool
Dynamic	7	Address Pool	Disabled	Pool 1

Result

Hosts IP addresses in the network 10.10.10.0 are translated to IP address in the range 172.16.131.2 to 172.16.131.10. When there are more requests for address translation than available addresses in Pool 1, the same address is used to satisfy subsequent requests, and PAT is used to distinguish between the hosts using the address.

Reasons that Cisco SDM Cannot Edit a NAT Rule

A previously configured NAT rule will be read-only and will not be configurable when a NAT static rule is configured with any of the following:

- The **inside source static** and **destination** Cisco IOS commands

- The **inside source static network** command with one of the keywords "extendable", "no-alias", or "no-payload"
- The **outside source static network** command with one of the keywords "extendable", "no-alias", or "no-payload"
- The **inside source static tcp** command with one of the keywords "no-alias" or "no-payload"
- The **inside source static udp** command with one of the keywords "no-alias" or "no-payload"
- The **outside source static tcp** command with one of the keywords "no-alias" or "no-payload"
- The **outside source static udp** command with one of the keywords "no-alias" or "no-payload"
- The **inside source static** command with one of the keywords "no-alias", "no-payload", "extendable", "redundancy", "route-map", or "vrf"
- The **outside source static** command with one of the keywords "no-alias", "no-payload", "extendable", or "add-route"
- The **inside source static** command with the keyword "esp"
- The **inside source static** command with the **interface** command

A NAT dynamic rule is configured with the Loopback interface

More About VPN

These topics contain more information about VPN, DMVPN, IPSec and IKE.

Cisco.com Resources

The following links provide TAC resources and other information on VPN issues.

- How Virtual Private Networks Work
- Dynamic Multipoint IPSec VPNs
- TAC-authored articles on IPSec
- TAC-authored articles on Cisco SDM

- Security and VPN Devices
- IPSecurity Troubleshooting–Understanding and Using Debug Commands
- Field Notices

More about VPN Connections and IPSec Policies

A VPN connection is an association between a router interface and an IPSec policy. The building block of an IPSec policy is the crypto map. A crypto map specifies the following: a transform set and other parameters to govern encryption, the identity of one or more peers, and an IPSec rule that specifies which traffic will be encrypted. An IPSec policy can contain multiple crypto maps.

The following diagram shows an interface (ATM 3/1.1) associated with an IPSec policy. The policy has three crypto maps, each specifying a different peer system. The ATM 3/1.1 interface is thus associated with three VPN connections.
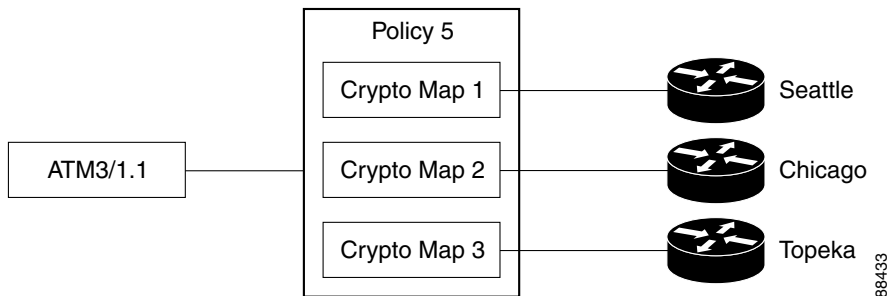
A crypto map can specify more than one peer for a connection. This may be done to provide redundancy. The following diagram shows the same interface and policy, but crypto map CM-3 specifies two peers: Topeka and Lawrence.
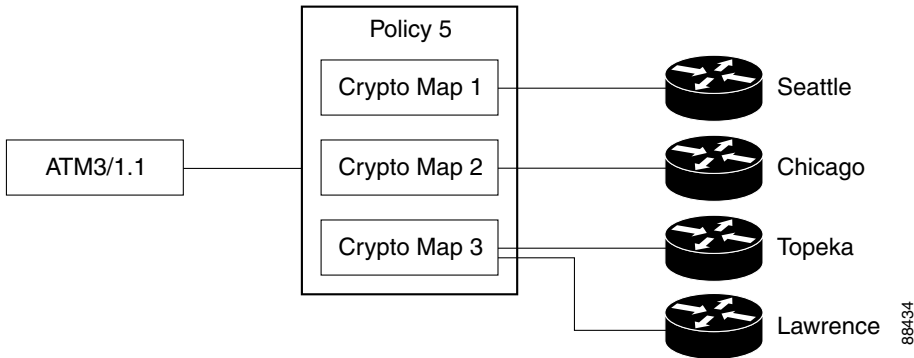
A router interface can be associated with only one IPSec policy. However, an IPSec policy can be associated with multiple router interfaces, and a crypto map can specify more than one peer for a connection. The following diagram shows two router interfaces associated with a policy, and a crypto map specifying two peers.
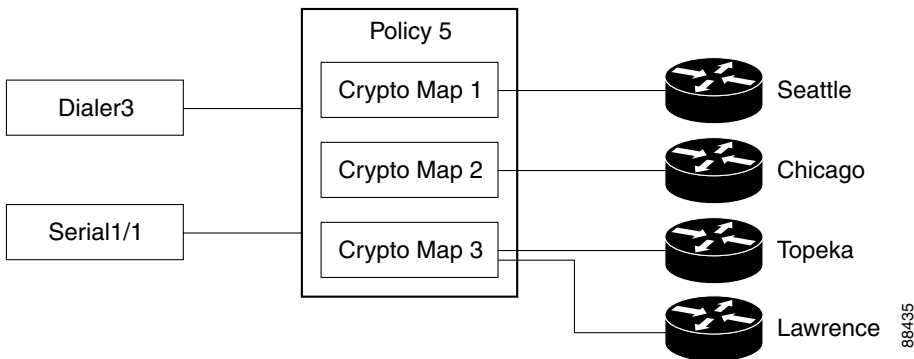
There are six VPN connections in this configuration, as both Dialer 3 and Serial 1/1 have connections to Seattle, Chicago, Topeka, and Lawrence. Cisco SDM would show the links to Topeka and Lawrence as one connection for both interfaces.

More About IKE

IKE handles the following tasks:

- Authentication
- Session Negotiation
- Key Exchange
- IPSec Tunnel Negotiation and Configuration

Authentication

Authentication is arguably the most important task that IKE accomplishes, and it certainly is the most complicated. Whenever you negotiate something, it is of utmost importance that you know with whom you are negotiating. IKE can use one of several methods to authenticate negotiating parties to each other.

- **Pre-shared Key**. IKE uses a hashing technique to ensure that only someone who possesses the same key could have sent the IKE packets.

- **DSS or RSA digital signatures**. IKE uses public-key digital-signature cryptography to verify that each party is whom he or she claims to be.

- **RSA encryption**. IKE uses one of two methods to encrypt enough of the negotiation to ensure that only a party with the correct private key could continue the negotiation.

Note Cisco SDM supports the pre-shared key method of authentication.

Session Negotiation

During session negotiation, IKE allows parties to negotiate how they will conduct authentication and how they will protect any future negotiations (that is, IPSec tunnel negotiation). The following items are negotiated:

- **Authentication Method**. This is one of the authentication methods listed above.

- **Key Exchange Algorithm**. This is a mathematical technique for securely exchanging cryptographic keys over a public medium (that is, Diffie-Hellman). The keys are used in the encryption and packet-signature algorithms.

- **Encryption Algorithm**: DES, 3DES, or AES
- **Packet Signature Algorithm**: MD5 or SHA-1

Key Exchange

IKE uses the negotiated key-exchange method (see "Session Negotiation" above) to create enough bits of cryptographic keying material to secure future transactions. This method ensures that each IKE session will be protected with a new, secure set of keys.

Authentication, session negotiation, and key exchange constitute phase 1 of an IKE negotiation.

IPSec Tunnel Negotiation and Configuration

After IKE has finished negotiating a secure method for exchanging information (phase 1), we use IKE to negotiate an IPSec tunnel. This is accomplished in IKE phase 2. In this exchange, IKE creates fresh keying material for the IPSec tunnel to use (either using the IKE phase 1 keys as a base or by performing a new key exchange). The encryption and authentication algorithms for this tunnel are also negotiated.

More About IKE Policies

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime-from the remote peer's policy will be used.

Allowable Transform Combinations

To define a transform set, you specify one to three transforms. Each transform represents an IPSec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

The following table lists the acceptable transform combination selections for the AH and ESP protocols.

AH Transform (*Pick up to one*)	ESP Encryption Transform (*Pick up to one*)	Authentication Transform (*Pick up to one*)	IP Compression Transform (*Pick up to one*)	Examples *(Total of 3 transforms allowed)*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	1. ah-md5-hmac 2. esp-3des and esp-md5-hmac 3. ah-sha-hmac, esp-des, and esp-sha-hmac

The following table describes each of the transforms.

Transform	Description
ah-md5-hmac	AH with the MD5 (HMAC variant) authentication algorithm.
ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm.
esp-des	ESP with the 56-bit DES encryption algorithm.
esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
esp-null	Null encryption algorithm.
esp-seal	ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm.

Transform	Description
esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm.
es-aes-128	ESP with Advanced Encryption Standard (AES). Encryption with a 128-bit key
esp-aes-192	ESP with AES. Encryption with a 192-bit key.
esp-aes-256	ESP with AES. Encryption with a 256-bit key.
esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm.
comp-lzs	IP compression with the LZS algorithm.

Examples

The following are examples of permissible transform combinations:

- ah-md5-hmac
- esp-des
- esp-3des and esp-md5-hmac
- ah-sha-hmac, esp-des, and esp-sha-hmac
- comp-lzs

Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only

A previously configured Serial interface or subinterface will be read-only and will not be configurable in the following cases:

- The interface is configured with the **encapsulation ppp** and **ppp multilink ...** Cisco IOS commands.
- The interface is configured with the **encapsulation hdlc** and **ip address negotiated** commands.
- The interface is part of a SERIAL_CSUDSU_56K WIC.
- The interface is part of a Sync/Async WIC configured with the **physical-layer async** command.

- The interface is configured with the **encapsulation frame-relay** command with an IP address on the main interface.

- The interface encapsulation is not "hdlc," "ppp," or "frame-relay."

- The **encapsulation frame-relay ...** command contains the **mfr ...** option.

- The interface is configured with the **encapsulation ppp** command, but the PPP configuration contains unsupported commands.

- The interface is configured with the **encapsulation frame-relay** and **frame-relay map ...** commands.

- The main interface is configured with the **encapsulation frame-relay** and **frame-relay interface-dlci ...** commands.

- The main interface is configured with the **encapsulation frame-relay** command and the subinterface is configured with the **frame-relay priority-dlci-group ...** command.

- The subinterface is configured with the **interface-dlci ...** command that contains any of the keywords "ppp," "protocol," or "switched."

- The subinterface type is "multipoint," instead of "point-to-point."

- The subinterface is configured with any encapsulation other than "frame-relay."

Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only

A previously configured ATM interface or subinterface will be read-only and will not be configurable in the following cases:

- It has a PVC with the **dialer pool-member** command.

- It has a PVC in which the protocol specified in the **protocol** command is not **ip.**

- It has a PVC with multiple **protocol ip** commands.

- The encapsulation on the PVC is neither "aal5mux," nor "aal5snap."

- If the encapsulation protocol on aal5mux is not "ip."

- If the IP Address is not configured on the PVC in the **protocol ip** command.

- If the "dial-on-demand" option is configured on the **pppoe-client** command.

- If there is more than 1 PVC configured on the interface.

- If the encapsulation on the associated dialer is blank or is not "ppp."

- If no IP address is configured on the associated dialer.

- If VPDN is required (which is determined dynamically from the Cisco IOS image) but is not configured for this connection.

- If the operating mode is "CO" on an SHDSL interface (ATM main interfaces only).

- If no IP address is configured on the interface and the interface is not configured for PPPoE (ATM subinterfaces only).

- The interface has an IP address but no associated PVC.

- The interface has a PVC but no associated IP address and is not configured for PPPoE.

- The **bridge-group** command is configured on the interface.

- If the main interface has one or move PVCs as well as one or more subinterfaces.

- If the main interface is not configurable (ATM subinterfaces only).

- It is a multipoint interface (ATM subinterfaces only).

Reasons Why an Ethernet Interface Configuration May Be Read-Only

A previously configured Ethernet LAN or WAN interface or will be read-only and will not be configurable in the following cases:

- If the LAN interface has been configured as a DHCP server, and has been configured with an IP-helper address.

Reasons Why an ISDN BRI Interface Configuration May Be Read-Only

A previously configured ISDN BRI interface will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the ISDN BRI interface.

- Encapsulation other than ppp is configured on the ISDN BRI interface.

- The **dialer-group** or **dialer string** command is configured on the ISDN BRI interface.

- **dialer pool-member** *<x>* is configured on the ISDN BRI interface, but the corresponding dialer interface *<x>* is not present.

- Multiple dialer pool-members are configured on the ISDN BRI interface.

- The **dialer map** command is configured on the ISDN BRI interface.

- Encapsulation other than ppp is configured on the dialer interface.

- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.

- **dialer-group** *<x>* is configured on the dialer interface, but the corresponding **dialer -list** *<x>* **protocol** command is not configured.

- **dialer idle-timeout** *<num>* with optional keyword (either/inbound) is configured on the dialer interface.

- **dialer string** command with optional keyword **class** is configured on the dialer interface.

- If using the ISDN BRI connection as a backup connection, once the backup configuration is through Cisco SDM, if any of the conditions below occur, the backup connection will be shown as read only:

  - The default route through the primary interface is removed

  - The backup interface default route is not configured

  - ip local policy is removed

  - **track /rtr** or **both** is not configured

  - route-map is removed

  - Access-list is removed or access-list is modified (for example, tracking ip address is modified)

- The Cisco SDM-supported interfaces are configured with unsupported configurations

- The primary interfaces are not supported by Cisco SDM

Reasons Why an Analog Modem Interface Configuration May Be Read-Only

A previously configured analog modem interface or will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the asynchronous interface.

- Encapsulation other than ppp is configured on the asynchronous interface.

- The **dialer-group** or **dialer string** command is configured on the asynchronous interface.

- Async mode **interactive** is configured on the asynchronous interface.

- **dialer pool-member** *<x>* is configured on the asynchronous interface, but the corresponding dialer interface *<x>* is not present.

- Multiple dialer pool-members are configured on the asynchronous interface.

- Encapsulation other than ppp is configured on the dialer interface.

- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.

- **dialer-group** *<x>* is configured on the dialer interface, but the corresponding **dialer -list** *<x>* **protocol** command is not configured.

- **dialer idle-timeout** *<num>* with optional keyword (either/inbound) is configured on the dialer interface.

- In line configuration collection mode, **modem inout** is not configured.

- In line configuration collection mode, **autoselect ppp** is not configured.

- If using the analog modem connection as a backup connection, once the backup configuration is through Cisco SDM, if any of the conditions below occur, the backup connection will be shown as read only:

  - The default route through the primary interface is removed

  - The backup interface default route is not configured

  - ip local policy is removed

- **track /rtr** or **both** is not configured

- route-map is removed

- Access-list is removed or access-list is modified (for example, tracking ip address is modified)

- The Cisco SDM-supported interfaces are configured with unsupported configurations

- The primary interfaces are not supported by Cisco SDM

Firewall Policy Use Case Scenario

For information on firewall policy management, including detailed deployment scenarios, see the document at the following link:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration_09186a0080230754.pdf

DMVPN Configuration Recommendations

This help topic contains recommendations on how you should proceed when configuring routers in a DMVPN.

Configure the Hub First

It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the Spoke Configuration feature available in the Summary window to generate a text file that contains a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

Assigning Spoke Addresses

All routers in the DMVPN must be in the same subnet. Therefore, the hub administrator must assign addresses in the subnet to the spoke routers so that address conflicts do not occur, and so that everyone is using the same subnet mask.

Recommendations for Configuring Routing Protocols for DMVPN

The following are guidelines that you should note when configuring routing protocols for DMVPN. You can choose to ignore these guidelines, but Cisco SDM has not been tested in scenarios outside the guidelines and may not be able to let you edit configurations within Cisco SDM after you enter them.

These recommendations are listed in best-choice order:

- If a routing process exists that advertises inside networks, use this process to advertise networks to the DMVPN.

- If a routing process exists that advertises tunnel networks for VPNs, for example GRE over IPSec tunnels, use this process to advertise the DMVPN networks.

- If a routing process exists that advertises networks for the WAN interfaces, then be sure to use an AS number or process ID that the WAN interfaces do not use to advertise networks.

- When you configure DMVPN routing information Cisco SDM checks whether the Autonomous System number (EIGRP) or area ID (OSPF) you enter is already used to advertise networks for the router's physical interface. If the value is already in use, Cisco SDM informs you of this and recommends that you either use a new value, or that you select a different routing protocol to advertise networks on the DMVPN.

Using Interfaces with Dialup Configurations

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected.

Ping the Hub Before You Start Spoke Configuration

Before configuring a spoke router, you should test connectivity to the hub by issuing the ping command. If the ping does not succeed, you must configure a route to the hub.

Cisco SDM White Papers

A number of white papers are available that describe how Cisco SDM can be used. These white papers are available at the following link.

http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/appnote/index.htm

Getting Started

Cisco Router and Security Device Manager (Cisco SDM) is an easy-to-use Internet browser-based software tool designed for configuring LAN, WAN, and security features on a router. Cisco SDM is designed for resellers and network administrators of small- to medium-sized businesses who are proficient in LAN fundamentals and basic network design.

For fast and efficient configuration of Ethernet networks, WAN connectivity, firewalls and Virtual Private Networks (VPNs), Cisco SDM prompts you through the setup process with wizards—sequenced screens that break down the configuration steps and provide you with explanatory text. You can then edit the basic configuration you created, for greater control over the router and the network. Cisco SDM requires no previous experience with Cisco devices or the Cisco command-line interface (CLI).

When you start Cisco SDM, it displays the Home Page, a window with system and configuration overview information that gives you important information about your router hardware and software. You can use this to determine what you want to configure. After you complete a configuration, Cisco SDM can help you test and troubleshoot it so that you can ensure that the configuration works.

Cisco SDM also features a Monitor mode, which enables you to observe router performance and gather statistics associated with configurations that you have made on the router.

What's New in this Release?

This release supports the following new features:

- The following hardware is now supported:

  - The Cisco 815 router.

  - The following cable modem network adapters:

    - HWIC-1CABLE-D

    - HWIC-1CABLE-E/J

  - The following Wide Area Application Services (WAAS) modules.

    - NME-WAE-502-K9

    - NME-WAE-522-K9

    - NME-WAE-302-K9

- Quality of Service over Dynamic Virtual Tunnel Interfaces Support—Cisco SDM enables you to associate QoS policies with DVTIs.

- QoS Policing, Queuing , and Shaping Support—Cisco SDM allows you to configure policing, queuing, and shaping in QoS policies.

  - For more information on QoS policing, refer to http://www.cisco.com/en/US/tech/tk543/tk545/tsd_technology_support_protocol_home.html

  - For more information on QoS queuing, refer to http://www.cisco.com/en/US/tech/tk543/tk544/tsd_technology_support_protocol_home.html

  - For more information on QoS shaping, refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a008022136e.html

- Easy VPN Enhancements— Cisco SDM supports the following Easy VPN enhancements:

  - Per-user AAA policy download with PKI.

  - Password aging.

  - Split DNS

  - Cisco Tunneling Control Protocol (cTCP).

- – Identical Addressing Support

  For more information on per-user AAA policy download with PKI, refer to
  http://www.cisco.com/en/US/products/ps6350/products_configuration_
  guide_chapter09186a0080455b6a.html

  For more information on password aging, split DNS, and cTCP, refer to
  http://www.cisco.com/en/US/products/ps6441/prod_bulletin09186a008
  04a84ad.html

  For more information about Identical Addressing Support, refer to
  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_fea
  ture_guide09186a00801541d5.html#wp1335885

- Zone-Based Policy Firewall (ZPF) Voice Protocol Support—Cisco SDM
  supports the SIP, H.323, and SCCP protocols.

- ZPF user interface enhancements.

- Wireless Application Enhancements—Cisco SDM supports the following
  enhancements:

  - – Advanced Encryption Standard-Counter Mode with Cipher Block
    Chaining Message Authentication Code Protocol (AES-CCMP)

  - – IEEE 802.1x Local Authentication Service for Extensible Authentication
    Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST).

  - – SSID Globalization

  - – Multiple Basic Service Set IDs (BSSID).

  - – Wireless Root, Non-Root Bridge & Universal Client Mode

  - – Multiple Encrypted VLANs

  - – VLAN assignment by name

  - – Wi-Fi Multimedia (WMM) elements.

- IPS user interface enhancements .

- Secure Socket Layer VPN (SSL VPN) enhancements—Cisco SDM now
  supports:

  - – URL Obfuscation

  - – Automatic download of the Thin Client applet

  - – Radius Accounting

- Application ACL
- Transcend Client

To find out more about this release, go to:

http://www.cisco.com/go/sdm

In the Support section, click the General Information link, and then click Release Notes.

Cisco IOS Versions Supported

To determine which Cisco IOS versions Cisco SDM supports, go to the following URL:

http://www.cisco.com/go/sdm

In the Support section, click the General Information link, and then click Release Notes.

Viewing Router Information

The Cisco Router and Security Device Manager (Cisco SDM) Monitor mode lets you view a current snapshot of information about your router, the router interfaces, the firewall, and any active VPN connections. You can also view any messages in the router event log.

Note The Monitor window is not dynamically updated with the latest information. To view any information that has changed since you brought up this window, you must click **Update**.

Monitor mode works by examining the router log and by viewing the results of Cisco IOS **show** commands. For Monitor mode functions that are based on log entries, such as firewall statistics, logging must be enabled. Logging is enabled by default by Cisco SDM, but you can change that setting using the **Additional Tasks > Router Properties > Logging** window. In addition, individual rules may need configuration so that they generate log events. For more information, see the help topic How Do I View Activity on My Firewall?

If you want to:	Do this:
View information about router interfaces.	From the toolbar, click **Monitor**, and then in the left frame, click **Interface Status**. From the Select Interface field select the interface for which you want to view information, then in the Available Items group, select the information you want to view. Then click **Show Details**.
View graphs of CPU or memory usage.	From the toolbar, click **Monitor**. The Overview page includes graphs of CPU usage and memory usage.
View information about the firewall.	From the toolbar, click **Monitor**, and then in the left frame, click **Firewall Status**.
View information about VPN Connections	From the toolbar, click **Monitor**, and then in the left frame, click **VPN Status**. Then select the tab for IPSec Tunnels, DMVPN Tunnels, Easy VPN Servers, or IKE SAs.
View messages in the router event log.	From the toolbar, click **Monitor**, and then in the left frame, click **Logging**.

Overview

The Monitor mode Overview screen displays an overview of your router activity and statistics, and serves as a summary of the information contained on the other Monitor mode screens. It contains the information described in this help topic.

Note If you do not see feature information described in this help topic on the Overview screen, the Cisco IOS image does not support the feature. For example, if the router is running a Cisco IOS image that does not support security features, the Firewall Status, and VPN status sections do not appear on the screen.

Launch Wireless Application Button

If the router has radio interfaces, you can click this button to monitor and configure radio interfaces. The Monitor Overview window provides interface status information for these interfaces, but radio interfaces are not listed in the Monitor Interface Status window.

This button does not appear if the router does not have radio interfaces.

Update Button

Retrieves current information from the router, updating statistics displayed by this screen.

Resource Status

Shows basic information about your router hardware and contains the following fields:

CPU Usage

Shows the percentage of CPU usage.

Memory Usage

Shows the percent of RAM usage.

Flash Usage

Shows the available flash over the amount of flash installed on the router.

Interface Status

Shows basic information about the interfaces installed on the router and their status.

> **Note** Only interface types supported by Cisco SDM are included in these statistics. Unsupported interfaces will not be counted.

Total Interface(s) Up

The total number of enabled (up) interfaces on the router.

Total Interface(s) Down

The total number of disabled (down) interfaces on the router.

Interface

The interface name.

IP

The IP address of the interface.

Status

The status of the interface, either Up, or Down.

Bandwidth Usage

The percent of interface bandwidth being used.

Description

Available description for the interface. Cisco SDM may add descriptions such as $FW_OUTSIDE$ or ETH_LAN.

Firewall Status Group

Shows basic information about the router resources and contains the following fields:

Number of Attempts Denied

Shows the number of log messages generated by connection attempts (by protocols such as Telnet, HTTP, ping, and others) rejected by the firewall. Note that in order for a log entry to be generated by a rejected connection attempt, the access rule that rejected the connection attempt must be configured to create log entries.

Firewall Log

If enabled, shows the number of firewall log entries.

QoS

The number of interfaces with an associated QoS policy.

VPN Status Group

Shows basic information about the router resources and contains the following fields:

Number of Open IKE SAs

Shows the number of IKE Security Associations (SAs) connections currently configured and running.

Number of Open IPSec Tunnels

Shows the number of IPSec Virtual Private Network (VPN) connections currently configured and running.

No. of DMVPN Clients

If the router is configured as a DMVPN hub, the number of DMVPN clients.

No. of Active VPN Clients

If the router is configured as an EasyVPN Server, this field shows the number of Easy VPN Remote clients.

NAC Status Group

Shows a basic snapshot of Network Admission Control (NAC) status on the router.

No. of NAC enabled interfaces field

The number of router interfaces on which NAC is enabled.

No. of validated hosts field

The number of hosts with posture agents that have been validated by the admissions control process.

Log Group

Shows basic information about the router resources and contains the following fields:

Total Log Entries

The total number of entries currently stored in the router log.

High Severity

The number of log entries stored that have a severity level of 2 or lower. These messages require immediate attention. Note that this list will be empty if you have no high severity messages.

Warning

The number of log entries stored that have a severity level of 3 or 4. These messages may indicate a problem with your network, but they do not likely require immediate attention.

Informational

The number of log entries stored that have a severity level of 6 or higher. These information messages signal normal network events.

Interface Status

The Interface Status screen displays the current status of the various interfaces on the router, and the numbers of packets, bytes, or data errors that have travelled through the selected interface. Statistics shown on this screen are cumulative since the last time the router was rebooted, the counters were reset, or the selected interface reset.

Monitor Interface and Stop Monitoring Button

Click this button to start or stop monitoring the selected interface. The button label changes based on whether Cisco SDM is monitoring the interface or not.

Test Connection Button

Click to test the selected connection. A dialog appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps you need to take to correct the problem.

Interface List

Select the interface for which you want to display statistics from this list. The list contains the name, IP address and subnet mask, the slot and port it is located in, and any Cisco SDM or user description entered.

Select Chart Types to Monitor Group

These check boxes are the data items for which Cisco SDM can show statistics on the selected interface. These data items are as follows:

- Packet Input—The number of packets received on the interface.

- Packet Output—The number of packets sent by the interface.

- Bandwidth Usage—The percent of bandwidth used by the interface, shown as a percentage value. Here is how bandwidth percentage is computed:

  Bandwidth percentage=(Kbps/bw) * 100,

  where

  bits per second= ((change in input+change in output) * 8) / poll interval

  Kbps= bits per second/1024

  bw=bandwidth capacity of the interface

  Because the differences in bytes input and bytes output can only be computed after the second view interval, the bandwidth percentage graph shows the correct bandwidth usage starting with the second view interval. See the View Interval section of this topic for polling intervals and view intervals.

- Bytes Input—The number of bytes received on the interface.

- Bytes Output—The number of bytes sent by the interface.

- Errors Input—The number of errors occurring while receiving data on the interface.

- Errors Output—The number of errors occurring while sending data from the interface.

- Packets flow—The number of packets in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

- Bytes flow—The number of bytes in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

- Total flow—The total number flows, from sources and destinations, for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

✏️ **Note** If the router Cisco IOS image does not support Netflow, the flow counters will not be available.

To view statistics for any of these items:

Step 1 Select the item(s) you want to view by checking the associated check box(es).

Step 2 Click **Monitor Interface** to see statistics for all selected data items.

Interface Status Area

View Interval

This pull-down field selects both the amount of data shown for each item and the frequency with which the data is updated. It has the following options

✏️ **Note** The polling frequencies listed are approximations and may differ slightly from the listed times.

- Real-time data every 10 sec. This option will continue polling the router for a maximum of two hours, resulting in approximately 120 data points.

- 10 minutes of data polled every 10 sec.

- 60 minutes of data, polled every 1 minute.

- 12 hours of data, polled every 10 minutes.

Note The last three options will retrieve a maximum of 60 data points. After 60 data points have been retrieved, Cisco SDM will continue to poll data, replacing the oldest data points with the newest ones.

Show Table/Hide Table

Click this button to show or hide the performance charts.

Reset button

Click this button to reset the interface statistic counts to zero.

Chart Area

This area shows the charts and simple numerical values for the data specified.

Note The last three options will retrieve a maximum of 30 data points. After 30 data points have been retrieved, Cisco SDM will continue to poll data, replacing the oldest data points with the newest ones.

Firewall Status

This window displays the following statistics about the firewall configured on the router:

- Number of Interfaces Configured for Inspection—The number of interfaces on the router that are configured to have traffic inspected by a firewall.

- Number of TCP Packets Count—The total number of TCP packets transmitted through the interfaces configured for inspection.

- Number of UDP Packets Count—The total number of UDP packets transmitted through the interfaces configured for inspection.

- Total number of active connections—The count of current sessions.

The Firewall Status window also displays active firewall sessions in a table with the following columns:

- Source IP Address—The IP address of the packet's origin host.

- Destination IP Address—The IP address of the packet's destination host.

- Protocol—The network protocol being examined.

- Match Count—The number of packets matching the firewall conditions.

Update button

Click this button to refresh the firewall sessions in the table and display the most current data from the router.

Zone-Based Policy Firewall Status

If the router runs a Cisco IOS image that supports the Zone-Based Policy Firewall feature, you can display the status of the firewall activity for each zone pair configured on the router.

Firewall Policy List Area

The firewall policy list area displays the policy name, source zone, and destination zone for each zone pair. The following table contains sample data for two zone pairs.

Zone Pair Name	Policy Name	Source Zone	Destination Zone
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

In this sample table there is a zone pair configured for traffic inbound to the DMZ, and traffic outbound from the DMZ.

Choose the zone pair that you want to display firewall statistics for.

View Interval

Choose one of the following options to specify how data should be collected:

- Real-time data every 10 sec—Data is reported every 10 seconds. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 10 seconds.

- 60 minutes of data polled every 1 minute—Data is reported every 1 minute. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 1 minute.

- 12 hours of data polled every 12 minutes—Data is reported every 12 minutes. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 12 minutes.

Monitor Policy

Click **Monitor Policy** to collect firewall data for the selected policy.

Stop Monitoring

Click **Stop Monitoring** to stop collecting firewall data .

Statistics Area

This area displays the firewall statistics for the selected zone pair. Control the display in this area by clicking on nodes in the tree on the left hand side. The following sections describe what you see when you click on each of the nodes.

Active Sessions

Clicking **Active Sessions** displays the traffic type, source IP address, and destination IP address for traffic that is inspected in the chosen zone pair.

Dropped Packets

For the chosen zone pair, clicking **Dropped Packets** displays a graph showing the cumulative number of dropped packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured to be dropped and logged in the Layer 4 policy map.

Allowed Packets

For the chosen zone pair, clicking **Allowed Packets** displays a graph showing the cumulative number of allowed packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured with the pass action in the Layer 4 policy map.

VPN Status

This window displays a tree of VPN connections that are possible on the router. You can choose one of the following VPN categories from the VPN connections tree:

- IPSec Tunnels
- DMVPN Tunnels
- Easy VPN Server
- IKE SAs
- SSL VPN Components

To view statistics on an active VPN category, choose it from the VPN connections tree.

IPSec Tunnels

This group displays statistics about each IPSec VPN that is configured on the router. Each row in the table represents one IPSec VPN. The columns in the table and the information they display are as follows:

- Interface column

    The WAN interface on the router on which the IPSec tunnel is active.

- Local IP column

    The IP address of the local IPSec interface.

- Remote IP column

    The IP address of the remote IPSec interface.

- Peer column

    The IP address of the remote peer.

- Tunnel Status

    The current status of the IPSec tunnel. Possible values are:

    - Up—The tunnel is active

    - Down—The tunnel is inactive due to an error or hardware failure.

- Encapsulation Packets column

  The number of packets encapsulated over the IPSec VPN connection.

- Decapsulation Packets column

  The number of packets decapsulated over the IPSec VPN connection.

- Send Error Packets column

  The number of errors that have occurred while sending packets.

- Receive Error Packets column

  The number of errors that have occurred while receiving packets.

- Encrypted Packets column

  The number of packets encrypted over the connection.

- Decrypted Packets column

  The number of packets decrypted over the connection.

Monitor Tunnel Button

Click to monitor the IPSec tunnel chosen in the IPSec Tunnel table. See Monitoring an IPSec Tunnel.

Test Tunnel.. Button

Click to test a selected VPN tunnel.The results of the test will be shown in another window.

Update button

Click this button to refresh the IPSec Tunnel table and display the most current data from the router.

Monitoring an IPSec Tunnel

To monitor an IPSec tunnel, follow these steps:

Step 1   Choose the tunnel you want to monitor in the IPSec Tunnel table.

Step 2   Choose the types of information you want to monitor by checking the checkboxes under **Select Item to Monitor**.

Step 3   Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

DMVPN Tunnels

This group displays the following statistics about Dynamic Multi-point VPN (DMVPN) tunnels. Each row reflects one VPN tunnel.

- Remote Subnet column

    The network address of the subnet to which the tunnel connects.

- Remote Tunnel IP column

    The IP address of the remote tunnel. This is the private IP address given the tunnel by the remote device.

- IP Public Interface of Remote Router column

    IP address of the public (outside) interface of the remote router.

- Status column

    The status of the DMVPN tunnel.

- Expiration column

    The time and date when the tunnel registration expires and the DMVPN tunnel will be shut down.

Monitor Tunnel Button

Click to monitor the DMVPN tunnel chosen in the DMVPN Tunnel table. See Monitoring a DMVPN Tunnel.

Update button

Click this button to refresh the DMVPN Tunnel table and display the most current data from the router.

Reset Button

Click to reset statistics counters for the tunnel list. Number of packets encapsulated and decapsulated, number of sent and received errors, and number of packets encrypted and decrypted are set to zero.

Monitoring a DMVPN Tunnel

To monitor a DMVPN tunnel, follow these steps:

Step 1 Choose the tunnel you want to monitor in the DMVPN Tunnel table.

Step 2 Choose the types of information you want to monitor by checking the checkboxes under **Select Item to Monitor**.

Step 3 Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

Easy VPN Server

This group displays the following information about each Easy VPN Server group:

- Total number of server clients (in upper right corner)
- Group Name
- Number of client connections

Group Details Button

Clicking **Group Details** shows the following information about the selected group.

- Group Name
- Key
- Pool Name
- DNS Servers
- WINS Servers

- Domain Name

- ACL

- Backup Servers

- Firewall-R-U-There

- Include local LAN

- Group lock

- Save password

- Maximum connections allowed for this group

- Maximum logins per user

Client Connections in this Group

This area shows the following information about the selected group.

- Public IP address

- Assigned IP address

- Encrypted Packets

- Decrypted Packets

- Dropped Outbound Packets

- Dropped Inbound Packets

- Status

Update button

Click this button to display the most current data from the router.

Disconnect button

- Choose a row in the table and click Disconnect to drop the connection with the client.

IKE SAs

This group displays the following statistics about each active IKE security association configured on the router:

- Source IP column

  The IP address of the peer originating the IKE SA.

- Destination IP column

  The IP address of the remote IKE peer.

- State column

  Describes the current state of IKE negotiations. The following states are possible:

  - MM_NO_STATE—The Internet Security Association and Key Management Protocol (ISAKMP) SA has been created but nothing else has happened yet.

  - MM_SA_SETUP—The peers have agreed on parameters for the ISAKMP SA.

  - MM_KEY_EXCH—The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.

  - MM_KEY_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.

  - AG_NO_STATE—The ISAKMP SA has been created but nothing else has happened yet.

  - AG_INIT_EXCH—The peers have done the first exchange in Aggressive mode but the SA is not authenticated.

  - AG_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.

  - QM_IDLE—The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent Quick mode exchanges.

- Update button—Click this button to refresh the IKE SA table and display the most current data from the router.

- Clear button—Select a row in the table and click Clear to clear the IKE SA connection.

SSL VPN Components

Clicking the VPN Status button in the monitoring window causes the router to begin monitoring SSL VPN activity. This window displays the data gathered for all SSL VPN contexts configured on the router.

By default, this data is refreshed every 10 seconds. If 10 seconds is too short an interval for you to view data before the next refresh, you can select an auto-refresh interval of **Real-time data every minute**.

Choose a context in the SSL VPN tree to view data for that context and data for the users who are configured for the context.

System Resources

The percentage of CPU and memory resources that SSL VPN traffic is using across all contexts is shown in this area.

Number of Connected Users

This graph shows the number of active users over time. The peak number of active users since monitoring began is displayed at the top of the graph area. The time that monitoring began is shown in the lower left-hand corner of the graph, and the current time is shown centered under the graph.

Tabbed Area

This area of the window displays gathered statistics in a series of tabs for easier viewing.

Click any of the links below for a description of the data the tab displays.

User Sessions

URL Mangling

Port Forwarding

CIFS

Full Tunnel

Note If a feature such as port forwarding or full tunnel has not been configured on the router, no data will be shown in the tab for that feature.

Some statistics are collected anew each time the router refreshes monitoring data. Other statistics, such as peak number of active users statistics, are collected at refresh time, but compared against the same data collected when monitoring began. Monitoring of all VPN activity, including SSL VPN, begins when you click the **VPN Status** button.

SSL VPN Context

This window shows the same types of information as the SSL VPN Components window but only shows the data gathered for the chosen context. For a description of the information displayed, click SSL VPN Components.

User Sessions

This tab displays the following information about SSL VPN user sessions.

- Active user sessions—The number of SSL VPN user sessions, of all traffic types, active since monitoring data was refreshed.

- Peak user sessions—The highest number of active SSL VPN user sessions since monitoring began.

- Active user TCP connections—The number of TCP-based SSL VPN user sessions active since monitoring data was refreshed.

- Session alloc failures—The number of session allocation failures that have occurred since monitoring began.

- VPN Session timeout—The number of VPN session timeouts that have occurred since monitoring began.

- User cleared VPN Sessions—The number of VPN sessions that have been cleared by users since monitoring began.

- AAA pending requests—The number of AAA requests that have been pending since monitoring data was refreshed.

- Peak time— The longest user session recorded since monitoring began.

- Terminated user sessions—The number of users sessions that have terminated since monitoring began.

- Authentication failures—The number of sessions that have failed to be authenticated since monitoring began.

- VPN Idle timeout—The number of VPN idle timeouts that have occurred since monitoring began.

- Exceeded context user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the context session limit had already been reached.

- Exceeded total user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the total session limit had already been reached.

URL Mangling

This tab displays data about URL mangling activities. For more information, refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Port Forwarding

This tab displays data gathered about port forwarding activities. For more information, refer to the command reference at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

This tab displays data gathered about CIFS requests, responses, and connections. For more information refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Full Tunnel

This tab displays information about full tunnel connections between SSL VPN clients and servers on the corporate intranet.

- Active tunnel connections—The number of active full tunnel connections since data was last refreshed. Data can be refreshed every 10 seconds, or every minute.

- Active connections peak time—The full tunnel connection of the longest duration since monitoring began.

- Peak active tunnel connections—The highest number of active full tunnel connections since monitoring began.

- Tunnel connection attempts failed—The number of full tunnel connection attempts that have failed since monitoring began.

- Tunnel connection attempts succeeded— The number of full tunnel connections successfully established since monitoring began.

Server:

- IP packets sent to server—The number of IP packets from full-tunnel clients that the router forwarded to servers on the corporate intranet.

- IP traffic sent to server in bytes—The amount of IP traffic, in bytes, forwarded from full-tunnel clients to servers on the corporate intranet.

- IP packets received from server—The number of IP packets that the router has received from servers with full-tunnel connections to clients.

- IP traffic received from server in bytes—The amount of IP traffic, in bytes, received from servers on the corporate intranet with full-tunnel connections to clients.

User List

This window displays user information for the context chosen in the SSL VPN Components tree. Because there can be multiple group polices configured for the context, each using their own URL list and server lists, this screen provides valuable information about how individual users are using their SSL VPN connections.

You can control individual use of the SSL VPN in this window by choosing a user and clicking the **Disconnect** button.

User List Area

This area lists all active users in all groups configured for this context. This area displays the following information:

- User Login Name—The username that is authenticated with the AAA server.

- Client IP address—The user's assigned SSL VPN IP address for this session. This IP address is drawn from the address pool configured for this context.

- Context—The SSL VPN context under which the group policy for this user has been configured.

- No. of connections—The number of active connections for the user. For example, the user might have a connection to a mail server, and might also be browsing files on another server in the network.

- Created—The time at which the session was created.

- Last used—The time at which the user last sent traffic over any active connection.

- Cisco Secure Desktop—True or False. Indicates whether Cisco Secure Desktop has been downloaded to the user's PC.

- Group name—The name of the group policy under which the user is configured. The group policy specifies the URL list, the services available to the users, the WINS servers available to resolve server names, and the servers that the users can see when browsing files on the corporate intranet.

- URL list name—The name of the URL list that appears on the user's portal page. The URL list is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.

- Idle timeout—The number of seconds that a session can remain idle before the router terminates it. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.

- Session timeout—The maximum number of seconds that a session can remain active before being terminated. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.

- Port forwarding list name—This value is configured for the group to which the user belongs. See Group Policy: Thin Client Tab for more information.

- WINS Name Service list name—This value is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.

Traffic Status

This window displays a tree of traffic types that can be monitored on an interface. Before any traffic type can be monitored, it must be enabled on at least one interface.

You can choose one of the following traffic types from the Traffic Status tree:

- Netflow Top Talkers
- QoS
- Application/Protocol Traffic

    This type uses Network-based application recognition (NBAR) to monitor traffic.

Netflow Top Talkers

If Netflow statistics have been enabled for at least one interface in **Configure > Interfaces and Connections > Edit Interface/Connection**, you can view Netflow statistics. Choose **Top N Traffic Flows > Top Protocols** or **Top N Traffic Flows > Top Talkers** (high-traffic sources) from the Traffic Status tree.

✎
Note   If the router Cisco IOS image does not support Netflow, the Netflow choices will not be available in the Traffic Status tree.

Top Protocols

This window displays a table with the following columns:

- Protocol—Protocol being examined.
- Total Flows—Total number of flows associated with that protocol.
- Flows/Sec—Active flows per second for the protocol.
- Packets/Flow—Packets transmitted per flow.
- Bytes/Packet—Bytes per transmitted packet.
- Packets/Sec—Packets transmitted per second.

Update Button

Updates the window with current information about the flows.

Top Talkers

This window displays a table with the following columns:

- **Source IP Address**—Source IP address of the top talker.

  Select a source IP address to see more information in **Flow status for the source address**.

- **Packets**—Total number of packets received from the source IP address.

- **Bytes**—Total number of bytes received from the source IP address.

- **Flows**—Number of flows associated with the source IP address.

> **Note** If Netflow top talkers is not enabled in **Configure > Additional Tasks > Router Properties > NetFlow**, then statistics for the top ten talkers are displayed.

Flow status for the source address

This table displays the following information about the flow associated with the selected source IP address:

- **Destination IP Address**—Target IP address of the top talker.

- **Protocols**—Protocols used in the packets exchanged with the destination IP address.

- **Number of Packets**—Number of packets exchanged with the destination IP address.

Update Button

Updates the window with current information about the flows.

QoS

The QoS Status window allows you to monitor the performance of the traffic on QoS configured interfaces (see Associating a QoS Policy With an Interface). This window also allows you to monitor bandwidth utilization and bytes-sent for interfaces with no QoS configuration. Monitoring inbound traffic on QoS interfaces shows the statistics only at a protocol level. Protocol-level statistics for non-QoS interfaces are collected for traffic in both directions.

This window allows you to monitor the following statistics:

- Bandwidth utilization for Cisco SDM defined traffic types

    - Bandwidth utilization per class under each traffic type

    - Bandwidth utilization for protocols under each class

    Bandwidth utilization is shown in Kbps.

- Total incoming and outgoing bytes for each traffic type

    - Incoming and outgoing bytes for each class defined under the traffic type

    - Incoming and outgoing bytes for each protocol for each class

    If the value is more than 1,000,000, then the graph may show the bytes as a multiple of 10^6. If the value is more than 1,000,000,000, then the graph may show the bytes as a multiple of 10^9.

- Packets dropped statistics for each traffic type

Interface—IP/Mask—Slot/Port—Description

This area lists the interfaces with associated QoS policies, their IP addresses and subnet masks, slot/port information if applicable, and available descriptions.

Select the interface that you want to monitor from this list.

View Interval

Select the interval at which statistics should be gathered:

- Now—Statistics are gathered when you click **Start Monitoring**.

- Every 1 minute—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-minute intervals.

- Every 5 minutes—Statistics are gathered when you click **Start Monitoring**, and refreshed at 5-minute intervals.

- Every 1 hour—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-hour intervals.

Start Monitoring

Click to start monitoring QoS statistics.

Select QoS Parameters for Monitoring

Select the traffic direction and type of statistics you want to monitor.

Direction
Click either **Input** or **Output**.

Statistics
Select one of the following

- Bandwidth

- Bytes

- Packets dropped

All Traffic—Real-Time—Business-Critical—Trivial

Cisco SDM displays statistics for all traffic classes in bar chart form, based on the type of statistic you selected. Cisco SDM displays a message instead of a bar chart if there are not adequate statistics for a particular traffic type.

Associating a QoS Policy With an Interface

Step 1   Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2   From the Interface List, choose the interface to which you want to associate a QoS policy.

Step 3   Click the **Edit** button.

Step 4   Click the **Application Service** tab.

Step 5 Choose a QoS policy from the **Inbound** drop-down list to associate with inbound traffic on the interface.

Step 6 Choose a QoS policy from the **Outbound** drop-down list to associate with outbound traffic on the interface.

Application/Protocol Traffic

This window allows you to monitor application and protocol traffic using Network-based application recognition (NBAR), a protocol and application discovery feature. NBAR is used to classify packets for more efficient handling of network traffic through a specific interface.

> **Note** If the router Cisco IOS image does not support NBAR, this status window will not be available.

Enable NBAR

To display the status of NBAR for a specific interface, NBAR must first be enabled on that interface. To enable NBAR, follow these steps:

Step 1 Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2 Choose the interface for which you want to enable NBAR from the Interface List.

Step 3 Click the **Edit** button.

Step 4 Click the **Application Service** tab.

Step 5 Check the **NBAR** checkbox.

NBAR Status

The NBAR status table displays the following statistics for the interface you choose from the **Select an Interface** drop-down list:

- Input Packet Count—The number of packets of the protocol shown incoming to the chosen interface.

- Output Packet Count—The number of packets of the protocol shown outgoing from the chosen interface.

- Bit rate (bps)—The speed, in bits per second, of traffic passing through the interface.

NAC Status

If NAC is configured on the router, Cisco SDM can display snapshot information about the NAC sessions on the router, the interfaces on which NAC is configured, and NAC statistics for the selected interface.

The top row in the window displays the number of active NAC sessions, the number of NAC sessions being initialized, and a button that allows you to clear all active and initializing NAC sessions

The window lists the router interfaces with associated NAC policies.

```
FastEthernet0/0   10.10.15.1/255.255.255.0   0
```

Clicking on an interface entry displays the information returned by posture agents installed on the hosts in the subnet for that interface. An example of the interface information follows:

```
10.10.10.5    Remote EAP Policy    Infected    12
```

10.10.10.1 is the host's IP address. Remote EAP Policy is the type of authentication policy that is in force. The host's current posture is Infected, and it has been 12 minutes since the host completed the admissions control process.

Note This area of the window contains no data if no posture information is returned by the hosts on the selected subnet.

The authentication types are:

- **Local Exception Policy**—An exception policy that is configured on the router is used to validate the host.

- **Remote EAP Policy**—The host returns a posture, and an exception policy assigned by an ACS server is used.

- **Remote Generic Access Policy**—The host does not have a posture agent installed, and the ACS server assigns an agentless host policy.

The posture agents on the hosts may return the following posture tokens:

- **Healthy**—The host is free of known viruses, and has the latest virus definition files.
- **Checkup**—The posture agent is determining if the latest virus definition files have been installed.
- **Quarantine**—The host does not have the latest virus definition files installed. The user is redirected to the specified remediation site that contains instructions for downloading the latest virus definition files.
- **Infected**—The host is infected with a known virus. The user is redirected to a remediation site to obtain virus definition file updates.
- **Unknown**—The host's posture is unknown.

Logging

Cisco SDM offers the following logs:

- Syslog—The router log.
- Firewall Log— If a firewall has been configured on the router, this log records entries generated by that firewall.
- Application Security Log—If an application firewall has been configured on the router, this log records entries generated by that firewall.
- SDEE Message Log—If SDEE has been configured on the router, this log records SDEE messages.

To open a log, click the tab with the log's name.

Syslog

The router contains a log of events categorized by severity level, like a UNIX syslog service.

> **Note** It is the router log that is displayed, even if log messages are being forwarded to a syslog server.

Logging Buffer

Shows whether or not the logging buffer and syslog logging are enabled. The text "Enabled" is displayed when both are enabled. The logging buffer reserves a specified amount of memory to retain log messages. The setting in this field is not preserved if your router is rebooted. The default settings for these fields are for the logging buffer to be enabled with 4096 bytes of memory.

Logging Hosts

Shows the IP address of any syslog hosts where log messages are being forwarded. This field is read-only. To configure the IP addresses of syslog hosts, use the **Additional Tasks > Router Properties > Logging** window.

Logging Level (Buffer)

Shows the logging level configured for the buffer on the router.

Number of Messages in Log

Shows the total number of messages stored in the router log.

Select a Logging Level to View

From this field, select the severity level of the messages that you want to view in the log. Changing the setting in this field causes the list of log messages to be refreshed.

Log

Displays all messages with the severity level specified in the Select a Logging Level to View field. Log events contains the following information:

- Severity Column

Shows the severity of the logging event. Severity is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

- – 0 - emergencies

  System unusable

- – 1- alerts

  Immediate action needed

- – 2 - critical

  Critical conditions

- – 3 - errors

  Error conditions

- – 4 - warnings

  Warning conditions

- – 5 - notifications

  Normal but significant condition

- – 6 - informational

  Informational messages only

- – 7 - debugging

  Debugging messages

- • Time Column

  Shows the time that the log event occurred.

- • Description Column

  Shows a description of the log event.

Update Button

Updates the window with current information about log details and the most current log entries.

Clear Log Button

Erases all messages from the log buffer on the router.

Search Button

Opens a search window. In the search window, enter text in the Search field and click the **Find** button to display all entries containing the search text. Searches are *not* case sensitive.

Firewall Log

The log entries shown in the top part of this window are determined by log messages generated by the firewall. In order for the firewall to generate log entries, you must configure individual access rules to generate log messages when they are invoked. For instructions on configuring access rules to cause log messages, see the help topic How Do I View Activity on My Firewall?

In order for firewall log entries to be collected, you must configure logging for the router. Go to **Additional Tasks** > **Router Properties** > **Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of debugging (7).

Firewall Log

The firewall log is displaed if the router is configured to maintain a log of connection attempts denied by the firewall.

Number of Attempts Denied by Firewall

Shows the number of connection attempts rejected by the firewall.

Attempts Denied by Firewall Table

Shows a list of connection attempts denied by the firewall. This table includes the following columns:

- Time column

    Shows the time that each denied connection attempt occurred.

- Description column

    Contains the following information about the denied attempt: log name, access rule name or number, service, source address, destination address, and number of packets. An example follows:

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

Update Button

Polls the router and updates the information shown on the screen with current information.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address—The IP address of the origin of the attack.

  A partial IP address can be entered.

- Destination IP Address—The IP address of the target of the attack.

  A partial IP address can be entered.

- Protocol—The network protocol used in the attack.

- Text—Any text found in the log entry.

Searches are *not* case sensitive.

View Top Attacks

From the View drop-down menu, choose one of the following ways to display information on top attacks:

- Top Attack Ports—Top attacks by target port.

- Top Attackers—by attacker IP address.

The top-attacks table below the View drop-down menu displays the top attack entries. If you choose Top Attack Ports from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Port Number—The target port.

- Number of attacks—The number of attacks against the target port.

- Number of packets denied—The number of packets denied access to the target port.

- View Details—A link that opens a window containing the full log of attacks against the chosen port.

If you choose Top Attackers from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Attacker's IP Address—The IP address from which the attacks are coming.

- Number of attacks—The number of attacks that have come from the IP address.

- Number of packets denied—The number of packets that have come from the IP address and were denied access.

- View Details—A link that opens a window containing the full log of the attacks from the chosen IP address.

Monitoring Firewall with a "Non-Administrator View" User Account

Firewall monitoring requires that Logging to Buffer be enabled on the router. If Logging to Buffer is not enabled, log in to Cisco SDM using an Administrator view account or a non-view based user account with privilege level 15 and configure logging.

To configure logging in Cisco SDM, go to **Additional Tasks > Router Properties > Logging**.

Application Security Log

If logging has been enabled, and you have specified that alarms be generated when the router encounters traffic from applications or protocols that you have specified, those alarms are collected in a log that can be viewed from this window.

In order for Application Security log entries to be collected, you must configure logging for the router. Go to **Additional Tasks > Router Properties > Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of **informational (6)**, or higher. If you have already configured logging for **debugging(7)**, the log will contain application security log messages.

The following is example log text:

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
```

```
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

Update Button

Updates the screen with current information about log details and the most current
log entries.

Search Button

Opens a search window. In the search window, enter text in the Search field and
click the **Find** button to display all entries containing the search text. Searches are
not case sensitive.

SDEE Message Log

This window lists the SDEE messages received by the router. SDEE messages are
generated when there are changes to IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All— SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

Update Button

Click to check for new SDEE messages.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address
- Destination IP Address
- Text

Searches are *not* case sensitive.

Time

The time the message was received.

Type

Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Description

Available description.

IPS Status

This window appears if the router is using a Cisco IOS image that supports IPS version 4.x or earlier. This window displays a table of IPS signature statistics, grouped by signature type. The following statistics are shown:

- **Signature ID**—Numerical signature identifier.
- **Description**—Description of the signature.
- **Risk Rating**—A a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- **Action**—The action that is to be taken when a packet matches a signature.
- **Source IP Address**—The IP address of the packet's origin host.
- **Destination IP Address**—The IP address of the packet's destination host.
- **Hits**—Number of matching packets.
- **Drop Counts**—Number of matching packets dropped.

To sort the signatures, click the column head with the name of signature statistic you want to sort by.

✎

Note   If you sort the signatures, the signatures may no longer be grouped by type. To restore the grouping of signatures by type, click the **Update** button.

Total Active Signatures

Displays the total number of signatures available that are active on your router.

Total Inactive Signatures

Displays the total number of signatures available that are inactive on your router.

Update Button

Click to check for and include the latest signature statistics.

Clear Button

Click to set set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Logging > SDEE Message Log**.

IPS Signature Statistics

This window is displayed if the router is using an IOS IPS 5.x configuration. Statistics are displayed for each enabled signature in the IOS IPS configuration. The top of the window displays signature totals to provide a snapshot of the signature configuration. The following totals are provided:

- Total Signatures
- Total Enabled Signatures
- Total Retired Signatures
- Total Compiled Signatures

Update and Clear Buttons

Click **Update** to check for and include the latest signature statistics. Click **Clear** to set set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Logging > SDEE Message Log**.

Signature List Area

The Signature ID, Description, number of hits, and drop count is shown for all signatures. If packet arrives that matches a signature, the source and destination IP addresses are listed as well.

IPS Alert Statistics

The IPS Alert Statistics window displays alert statistics in a color-coded format for easy recognition. The top part of the screen displays a legend that explains the use of colors in the display.

Color	Explanation
RED	The event that generated the alert has a high Risk Rating (RR) in the range of 70 to 100.
MAGENTA	The event that generated the alert has a medium Risk Rating (RR) in the range of 40 to 69.
BLUE	The event that generated the alert has a low Risk Rating (RR) in the range of 0 to 39.

By clicking on a column heading, you sort the display based on the values of that parameter. For example, by clicking on the **Signature ID** heading, you sort the display in ascending or descending numerical order of signature IDs. Each column is described in the following list:

- **Signature ID**—Numerical signature identifier.
- **Description**—Description of the signature.
- Risk Rating—A value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- Event Action—The action that IOS IPS is to take when an event matching the signature occurs.
- Source IP Address—The IP address from which the packet originated.
- Destination IP Address—The IP address to which the packet was addressed. If the packet is malicious, the Destination IP address can be considered the target.
- Hits—Number of matching packets.
- Drop Count—The number of matching packets dropped.
- Engine—The signature engine associated with the signature.

802.1x Authentication Status

802.1x Authentication on Interfaces Area

Interface

802.1x Authentication

Reauthentication

802.1x Clients Area

Client MAC Address

Authentication Status

Interface

File Menu Commands

The following options are available from the Cisco Router and Security Device Manager (Cisco SDM) File menu.

Save Running Config to PC

Saves the router's running configuration file to a text file on the PC.

Deliver Configuration to Router

This window lets you deliver to the router any configuration changes that you have made using Cisco SDM. Note that any changes to the configuration that you made using Cisco SDM will not affect the router until you deliver the configuration.

Save Running Config to Router's Startup Config

Check this check box to cause Cisco SDM to save the configuration shown in the window to both the router running configuration file and the startup file. The running configuration file is temporary—it is erased when the router is rebooted. Saving the configuration to the router startup configuration causes the configuration changes to be retained after a reboot.

If Cisco SDM is being used to configure a Cisco 7000 router, the check box **Save running config. to router's startup config.** will be disabled if there are **boot network** or **boot host** commands present with **service config** commands in the running configuration.

Cancel

Click this button to discard the configuration change and close the Cisco SDM Deliver to Router dialog box.

Save to File

Click this button to save the configuration changes shown in the window to a text file.

Write to Startup Config

Writes the router's running configuration file to the router startup configuration.

If Cisco SDM is being used to configure a Cisco 7000 router, this menu item will be disabled if there are **boot network** or **boot host** commands present with **service config** commands in the running configuration.

Reset to Factory Defaults

See Reset to Factory Defaults.

File Management

This window allows you to view and manage the file system on your Cisco router flash memory and on USB flash devices connected to that router. Only DOSFS file systems can be viewed and managed in this window.

The left side of window displays an expandable tree representing the directory system on your Cisco router flash memory and on USB flash devices connected to that router.

The right side of the window displays a list of the names of the files and directories found in the directory that is chosen in the left side of the window. It also shows the size of each file in bytes, and the date and time each file and directory was last modified.

You can choose a file or directory in the list on the right side of the window and then choose one of the commands above the list.

Directories (folders) can be renamed or deleted. Single or multiple files can be copied, pasted, or deleted, and single files can be renamed. However, the following restrictions apply:

- Files cannot be pasted into the directory from which they were copied.

- If Cisco SDM is invoked from your router flash, then Cisco SDM files can not be deleted.

  You can delete Cisco SDM files that are copies or if Cisco SDM is invoked from a PC.

- If Cisco SDM is invoked from your router flash, then Cisco SDM files can not be renamed.

  You can rename Cisco SDM files that are copies or if Cisco SDM is invoked from a PC.

- If Cisco SDM is invoked from your router flash, then you can not replace (copy over with a file of the same name) an Cisco SDM file.

  You can replace Cisco SDM files that are copies or if Cisco SDM is invoked from a PC.

- Cisco IOS software files can not be renamed.

- Directories (folders) can not be copied.

If your router is booted from a tftp server, then no file operation restrictions are in effect.

Refresh Button

Click the **Refresh** button to fetch a new image of the directories and files from your Cisco router flash memory and from USB flash devices connected to that router.

Format Button

Click the **Format** button to reformat your Cisco router flash memory or to reformat a USB flash device connected to that router. The **Format** button is enabled only if an icon representing your Cisco router flash memory or a USB flash device is chosen in the left side of the window.

⚠

Caution   Reformatting your Cisco router flash memory or a USB flash device connected to that router will *erase* all of the files in the file system.

New Folder Button

Click the **New Folder** button to create a new directory in the directory that is chosen in the left side of the window. Folder names cannot contain spaces or question marks ("?").

Load File From PC Button

Click the **Load File From PC** button to open a file-selection window on the local PC. Choose a file to save to the chosen directory on your Cisco router flash memory or on a USB flash device connected to that router. Cisco SDM files and files with names containing spaces cannot be loaded using Load File From PC.

Cisco SDM files, such as Cisco SDM.tar, can not be loaded using Load File From PC. Cisco SDM files should be loaded using **Tools > Update SDM**.

If you use Load File From PC to load a boot image file, it can not be saved to the current boot image file directory.

Copy Button

Choose a file from the right side of the window and click the **Copy** button to copy the file.

Paste Button

After you click the **Copy** button to copy a file, click the **Paste** button to place the copy of the file in a different directory. Choose a target directory from the left side of the window. You cannot place a copy of the file in the same directory as the original file.

Rename Button

Choose a file or directory from the right side of the window and click the **Rename** button to change its name. Names cannot contain spaces or question marks ("?").

Delete Button

Choose a file or directory from the right side of the window and click the **Delete** button to delete it. A file with the no-write icon next to its name cannot be deleted.

Name

Click **Name** to order the files and directories alphabetically based on name. Clicking **Name** again will reverse the order.

Size

Click **Size** to order the files and directories by size. Directories always have a size of zero bytes, even if they are not empty. Clicking **Size** again will reverse the order.

Time Modified

Click **Time Modified** to order the files and directories based on modification date and time. Clicking **Time Modified** again will reverse the order.

Rename

This window allows you to rename a file on your Cisco router flash memory or on USB flash devices connected to that router.

Enter the new filename in the New Name field. The path to the location of the file is displayed above the New Name field.

New Folder

This window allows you to name and create a new folder in the directory system on your Cisco router flash memory and on USB flash devices connected to that router.

Enter the name of the new folder in the Folder Name field. The path to the location of the new folder is displayed above the Folder Name field.

Save SDF to PC

If you are working in IPS, you can save the signature definition file (SDF) that you are working on to your PC. Navigate to the directory in which you want to save the file, and click **Save**.

Exit

Exits Cisco Router and Security Device Manager.

Unable to perform squeeze flash

This window appears when your router is unable to perform a squeeze flash operation because an **erase flash:** operation has never been performed on the router. This help topic explains how to download the files you need before performing the **erase flash:** operation, how to execute **erase flash:**, and how to load files back onto the router and reconnect to Cisco SDM afterward.

Executing the **erase flash:** command will remove Cisco SDM and the Cisco IOS image from the router's Flash memory, and you will lose your connection to the router. You should print the contents of this help topic so that you can use the instructions to obtain a Cisco IOS image and SDM.tar from Cisco.com, and install them on the router.

Step 1   Ensure that the router will not lose power. If the router loses power after an **erase flash:** operation, there will be no Cisco IOS image in memory.

> **Note**   If the router does lose power after the erase flash operation, you can use the procedure at the following link to recover:
> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis37 00/sw_conf/37_swcf/appendc.htm#xtocid11

Step 2   Save the router's running configuration to a file on the PC by clicking **File > Save Running Config to PC**, and entering a filename.

Step 3   Prepare a TFTP server to which you can save files and copy them over to the router. You must have write access to the TFTP server. Your PC can be used for this purpose if it has a TFTP server program.

Step 4   Use the **tftpcopy** command to copy the Cisco IOS image, the SDM.tar file, and the SDM.shtml file from Flash memory to a TFTP server:

copy flash: tftp://*tftp-server-address*/*filename*

Example:

```
copy flash: tftp://10.10.10.3/SDM.tar
```

> **Note**   If you prefer to download a Cisco IOS image, the SDM.tar file, and the SDM.shtml file, follow these instructions to use an Internet connection to download an Cisco SDM-supported Cisco IOS image, the SDM.tar file, and the SDM.shtml file. Then place those files on a TFTP server.

   a. Click the following link to obtain a Cisco IOS image from the Cisco Software Center:

   http://www.cisco.com/kobayashi/sw-center/

   b. Obtain an image that supports the features you want on the 12.2(11)T release or later. Save the file to the TFTP server that is accessible from the router.

   c. Use the following link to obtain the SDM.tar and SDM.shtml files. Then save SDM.tar and SDM.shtml to the TFTP server.

   http://www.cisco.com/go/sdm

Step 5   From the PC, log on to the router using Telnet, and enter Enable mode.

Step 6   Enter the command **erase flash:**, and confirm. The router's IOS image, configuration file, the SDM.tar file, and the SDM.shtml file are removed from non-volatile RAM (NVRAM).

Step 7   Use the **tftpcopy** command to first copy the IOS image and then SDM.tar from the TFTP server to the router:

copy tftp://*tftp-server-address*/*filename* **flash:**

Example:

```
copy tftp://10.10.10.3/ios_image_name flash:
! Replace ios_image_name with actual name of IOS image
copy tftp://10.10.10.3/SDM.tar flash:
```

Step 8   Start your web browser, and reconnect to Cisco SDM, using the same IP address you used when you started the Cisco SDM session.

Now that an **erase flash:** has been performed on the router, you will be able to execute the **squeeze flash** command when necessary.

Edit Menu Commands

The following options are available from the Cisco Router and Security Device Manager (Cisco SDM) Edit menu.

Preferences

This screen lets you configure the following Cisco Router and Security Device Manager options:

Preview commands before delivering to router

Choose this option if you want Cisco SDM to display a list of the Cisco IOS configuration commands generated before the commands are sent to the router.

Save signature file to Flash

Choose this option if you want the signature definition file (SDF) that you are working on to be saved to router flash when you click **Apply Changes**.

Confirm before exiting Cisco SDM

This is Cisco SDM default behavior. Select this option if you would like Cisco SDM to display a dialog box asking for confirmation when you exit Cisco SDM.

Continue monitoring interface status when switching mode/task

This is Cisco SDM default behavior. Cisco SDM begins monitoring interface status when you click **Monitor** and select **Interface status**. To have Cisco SDM continue monitoring the interface even if you leave Monitor mode and perform other tasks in Cisco SDM, select this check box and specify the maximum number of interfaces you want Cisco SDM to monitor. The default maximum number of interfaces to monitor is 4.

View Menu Commands

The following options are available from the Cisco Router and Security Device Manager (Cisco SDM) View menu.

Home

Displays the Cisco SDM Home page which provides information about router hardware, software, and LAN, WAN, Firewall, and VPN configurations.

Configure

Displays the Cisco SDM Tasks bar, which allows you to perform guided and manual configurations for Interfaces and Connections, Firewalls and ACLs, VPNs Routing, and other tasks.

Monitor

Displays the Cisco SDM Monitor window, which lets you view statistics about your router and network.

Running Config

Displays the router's running configuration.

Show Commands

Displays the Show Commands dialog box, which lets you issue Cisco IOS **show** commands to the router, view the output, and save the output to your PC. The output file is saved with the default filename show_<*command*>[*router_ip_address*].

The Show Commands dialog box can display the output from the following **show** commands:

- **show flash**—Shows the contents of the router Flash memory.
- **show startup-config**—Shows the router startup configuration file.
- **show access-lists**—Shows all of the Access Control Lists (ACLs) commands currently configured on the router.
- **show diag**—Shows information about the hardware installed in the router.
- **show interfaces**—Shows information about the configuration of each interface and about the packets transferred over the interface.
- **show protocols**—Shows information about the network protocols configured on each interface.
- **show version**—Shows information about the version of Cisco IOS software running on the router.
- **show tech-support**—Shows the output from all of the other **show** commands.
- **show environment**—Shows information about the router power supply. This command may not appear in the **Show Commands** drop-down list if not supported by your router.

Cisco SDM Default Rules

The Cisco SDM Default Rules screen displays a list of all of the default rules configured by Cisco SDM. The screen is organized with a tree on the left side of the screen displaying options for Access Rules, Firewall, VPN - IKE Policy, and VPN - Transform Sets. To view the default rules for these options, click the option in the tree, and the default rules for that option are displayed on the right. For more information about the rules, see the option descriptions that follow.

Access Rules

Shows all of the default Access Control List (ACL) rules and a brief description of each.

Firewall

Shows Cisco SDM's default Application Security policies. Choose the security policy that you want to view from the list in the upper right corner of the window.

- SDM_HIGH—This policy prevents the use of Instant Messaging and Point-to-Point applications on the network. It monitors HTTP and e-mail traffic and drops traffic that does not comply with the protocol it uses. It returns other TCP and UPD traffic for sessions started inside the firewall.

- SDM_MEDIUM—This policy monitors the use of Instant Messaging and Point-to-Point applications, and HTTP and email traffic. It returns other TCP and UPD traffic for sessions started inside the firewall.

- SDM_LOW—This policy does not monitor application traffic. It returns other TCP and UPD traffic for sessions started inside the firewall.

VPN - IKE Policy

Shows the default Internet Key Exchange (IKE) policies.

VPN - Transform Sets

Shows the default IP Security (IPSec) transform sets.

Refresh

Reloads configuration information from the router. If there are any undelivered commands, Cisco SDM displays a message window telling you that if you refresh, you will lose undelivered commands. If you want to deliver the commands. click **No** in this window, and then click **Deliver** on the Cisco SDM toolbar.

Tools Menu Commands

The following options are available from the Cisco Router and Security Device Manager (Cisco SDM) Tools menu.

Ping

Displays the Ping dialog box, which lets you send a ping message to another network device. See Generate Mirror... for information on how to use the Ping window.

Telnet

Displays the Windows Telnet dialog box, letting you connect to your router and access the Cisco IOS command-line interface (CLI) using the Telnet protocol.

Security Audit

Displays the Cisco SDM Security Audit screen. See Security Audit for more information.

USB Token PIN Settings

The USB Token PIN Settings dialog box allows you to set PINs for USB tokens connected to your router.

Select a PIN Type

Choose **User PIN** to set a user PIN, or **Admin PIN** to set an administrator PIN.

A user PIN is used to log into a router. If you connect a USB token to a router, and the token's name and user PIN match an entry in **Configure > VPN > VPN Components > Public Key Infrastructure > USB Tokens**, you are automatically logged into that router.

An administrator PIN is used to manage USB token settings using the manufacturer's software. Cisco SDM allows you to change the administrator PIN for a USB token if you can supply the current administrator PIN.

Token Name

Enter the USB token's name.

The token's name is set by the manufacturer. For example, USB tokens manufactured by Aladdin Knowledge Systems are named eToken.

You can also use the name "usbtoken$x$", where x is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

Current PIN

Enter the existing user or administrator PIN. If you do not know the existing PIN, you must use the USB token manufacturer's software to find it.

New PIN

Enter a new PIN for the USB token. The existing PIN will be replaced by the new PIN. The new PIN must be at least 4 digits long.

Confirm PIN

Reenter the new PIN to confirm it.

Save the New PIN to Router

Check the **Save the new PIN to router** checkbox if you want to save the new PIN as an entry in **Configure > VPN > VPN Components > Public Key Infrastructure > USB Tokens**. If an entry with the same name already exists in **Configure > VPN > VPN Components > Public Key Infrastructure > USB Tokens**, it is replaced with the new one.

The **Save the new PIN to router** checkbox is available only for user PINs.

Wireless Application

If the router has radio interfaces, you can launch the Wireless Application to configure and monitor those interfaces. Cisco SDM can help you configure and display the IP address or bridging details about a radio interface, but you must use the Wireless Application to set other configuration parameters.

Update Cisco SDM

You can have Cisco SDM obtain and install an update automatically.

Update Cisco SDM from Cisco.com

You can update Cisco SDM directly from Cisco.com. Cisco SDM checks Cisco.com for the versions available and informs you if there is a version newer than the one currently running on the router. You can then update Cisco SDM using the Update wizard.

To update Cisco SDM from Cisco.com:

Step 1   Select Update Cisco SDM from Cisco.com from the Tools menu. Selecting this option starts the update wizard.

Step 2   Use the update wizard to obtain the Cisco SDM files and copy them to your router.

Update Cisco SDM from Local PC

You can update Cisco SDM using an SDM.zip file you have downloaded from Cisco.com. Cisco SDM provides an update wizard that will copy the necessary files to your router.

To update Cisco SDM from the PC you are using to run Cisco SDM follow these steps:

Step 1   Download the file sdm-v*nn*.zip from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

If there is more than one Cisco SDM .zip file, obtain the copy with the highest version number.

Step 2   Use the update wizard to copy the Cisco SDM files from your PC to the router.

Update Cisco SDM from CD

If you have the Cisco SDM CD, you can use it to update Cisco SDM on your router. To do so, follow these steps:

Step 1   Place the Cisco SDM CD in the CD drive on your PC.

Step 2   Select **Update Cisco SDM from CD**, and click **Update Cisco SDM** in the General Instructions window after reading the text.

Step 3   Cisco SDM will enable you to locate the file SDM-Updates.xml on the CD. When you locate the file, click **Open**.

Step 4   Follow the instructions in the installation wizard.

CCO Login

You must provide a CCO login and password to access this web page. Provide a username and password, and then click OK.

If you do not have a CCO login and password, you can obtain one by opening a web browser and going to the Cisco website at the following link:

http://www.cisco.com

When the webpage opens, click Register and provide the necessary information to obtain a username and password. Then, try this operation again.

CCO Login

Help Menu Commands

The following options are available from the Cisco Router and Security Device Manager (Cisco SDM) Help menu.

Help Topics

Displays the Cisco SDM online help. The Cisco SDM online help Table of Contents appears in the left frame of the help.

Cisco SDM on CCO

Opens up a browser and displays the Cisco SDM page on the Cisco.com website.

Hardware/Software Matrix

Opens up a browser and displays a matrix of Cisco router models and Cisco IOS image versions to guide you in selecting compatible Cisco IOS image software. A Cisco Connection Online username and password are required to access the matrix.

About this router...

Displays hardware and software information about the router on which Cisco SDM is running.

About Cisco SDM

Displays version information about Cisco SDM.

GLOSSARY

Symbols and Numerics

3DES
Triple DES. An encryption algorithm that uses three 56-bit DES encryption keys (effectively 168 bits) in quick succession. An alternative 3DES version uses just two 56-bit DES keys, but uses one of them twice, resulting effectively in a 112-bit key length. Legal for use only in the United States. See DES.

802.1x
802.1x is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access and apply traffic policy, based on user or machine identity.

A

AAA
Authentication, Authorization, and Accounting. Pronounced "triple-A."

AAL5-SNAP
ATM Adaptation Layer 5 Subnetwork Access Protocol.

AAL5-MUX
ATM Adaptation Layer 5 Multiplexing.

access control, access control rule
information entered into the configuration which allows you to specify what type of traffic to permit or deny into an the interface. By default, traffic that is not explicitly permitted is denied. Access control rules are composed of access control entries (ACEs).

ACE
access control entry. An entry in an ACL that specifies a source host or network and whether or not traffic from that host is permitted or denied. An ACE can also specify a destination host or network, and the type of traffic.

ACL
access control list. Information on a device that specifies which entities are permitted to access that device or the networks behind that device. Access control lists consist of one or more access control entries (ACE).

ACS
Cisco Secure Access Control Server. Cisco software that can implement a RADIUS server or a TACACS+ server. The ACS is used to store policy databases used by Easy VPN, NAC and other features to control access to the network.

address translation
The translation of a network address and/or port to another network address/or port. See also IP address, NAT, PAT, Static PAT.

ADSL
asymmetric digital subscriber line.

aggressive mode
A mode of establishing ISAKMP SAs that simplifies IKE authentication negotiation (phase 1) between two or more IPSec peers. Aggressive mode is faster than main mode, but is not as secure. See main mode, quick mode.

AES
Advanced Encryption Standard

AES-CCMP
Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security.

AH
Authentication Header. This is an older IPSec protocol that is less important in most networks than ESP. AH provides authentication services but does not provide encryption services. It is provided to ensure compatibility with IPSec peers that do not support ESP, which provides both authentication and encryption.

AH-MD5-HMAC
Authentication Header with the MD5 (HMAC variant) hash algorithm.

AH-SHA-HMAC
Authentication Header with the SHA (HMAC variant) hash algorithm.

AHP
Authentication Header Protocol. A protocol that provides source host authentication, and data integrity. AHP does not provide secrecy.

algorithm	A logical sequence of steps for solving a problem. Security algorithms pertain to either data encryption or authentication.
	DES and 3DES are two examples of data encryption algorithms.
	Examples of encryption-decryption algorithms include block cipher, CBC, null cipher, and stream cipher.
	Authentication algorithms include hashes such as MD5 and SHA.
AMI	alternate mark inversion.
ARP	Address Resolution Protocol—A low-level TCP/IP protocol that maps a node hardware address (called a *MAC address*) to its IP address.
ASA	Adaptive Security Algorithm. Allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.
asymmetric encryption	Also called *public key systems*, this approach allows anyone to obtain access to anyone else's public key and therefore send an encrypted message to that person using the public key.
asymmetric keys	A pair of mathematically related cryptographic keys. The public key encrypts information that only the private key can decrypt, and vice versa. Additionally, the private key signs data that only the public key can authenticate.
ATM	Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, and data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays.
authenticate	To establish the truth of an identity.
authentication	In security, the verification of the identity of a person or process. Authentication establishes the integrity of a data stream, ensuring that it was not tampered with in transit, and providing confirmation of the data stream's origin.

B

BC Committed Burst. BC is a QoS policing parameter that specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns.

BE Excess Burst. BC is a QoS policing parameter that specifies how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.

BOOTP Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.

BSSID Basic Service Set Identifier. BSSIDs are identifiers used in 802.11g radios. They are similar to MAC addresses

burst rate The number of bytes that a traffic burst must not exceed.

C

C3PL Cisco Common Classification Policy Language. C3PL is a structured replacement for feature-specific configuration commands and allows configurable functionality to be expressed in terms of an event, a condition, and an action.

CA Certification Authority. A trusted third-party entity that issues and/or revokes digital certificates. Sometimes referred to as a *notary* or a *certifying authority.* Within a given CA's domain, each device needs only its own certificate and the CA's public key to authenticate every other device in that domain.

CA certificate A digital certificate granted to one certification authority (CA) by another certification authority.

CA server Certification Authority server. A network host that is used to issue and/or revoke digital certificates.

cache A temporary repository of information accumulated from previous task executions that can be reused, decreasing the time required to perform the tasks.

CBAC Context-based Access Control. Protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC scrutinizes both source and destination addresses and tracks each application connection status.

CBWFQ Class-Based Weighted Fair Queuing. CBWFQ provides support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces.

CDP Cisco Discovery Protocol. A media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN.

CDP Certificate Revocation List Distribution Point. A location from with a Certificate Revocation List can be retrieved. A CDP is usually an HTTP or LDAP URL

CEP Certificate Enrollment Protocol. A certificate management protocol. CEP is an early implementation of Certificate Request Syntax (CRS), a standard proposed to the Internet Engineering Task Force (IETF). CEP specifies how a device communicates with a CA, including how to retrieve the public key of the CA, how to enroll a device with the CA, and how to retrieve a certificate revocation list (CRL). CEP uses PKCS (Public Key Cryptography Standards) 7 and 10 as key component technologies. The public key infrastructure working group (PKIX) of the IETF is working to standardize a protocol for these functions, either CRS or an equivalent. When an IETF standard is stable, Cisco will add support for it. CEP was jointly developed by Cisco Systems and VeriSign, Inc.

certificate See digital certificate.

certificate identity An X.509 certificate contains within it information regarding the identity of whichever device or entity possesses that certificate. The identification information is then examined during each subsequent instance of peer verification and authentication. However, certificate identities can be vulnerable to spoofing attacks.

CET	Cisco Encryption Technology. Proprietary network layer encryption introduced in Cisco IOS Release 11.2. CET provides network data encryption at the IP packet level and implements the following standards: DH, DSS, and 40- and 56-bit DES.
CHAP	Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. The router or access server then determines whether that user is allowed access. See also PAP.
chargen	Character Generation. Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time the client sends a datagram.
checksum	Computational method for checking the integrity of transmitted data, computed from a sequence of octets taken through a series of arithmetic operations. The recipient recomputes the value and compares it for verification.
Cisco SDM	Cisco Router and Security Device Manager. Cisco SDM is an Internet browser-based software tool designed to configure LAN, WAN, and security features on a router. See Getting Started for more information.
cipher	An encryption-decryption algorithm.
ciphertext	Encrypted, unreadable data, prior to its decryption.
CIR	Committed Information Rate. A configured long-term average committed rate to enforce.
class map	Used by zone-based firewall policies to specify traffic that is to be handled according to the actions specified in a policy map. A class map can specify a type of traffic, and can also specify an ACL to define the source and destinaton of the traffic.
clear channel	A clear channel is one through which non-encrypted traffic can flow. Clear channels place no security restrictions on transmitted data.
cleartext	Decrypted text. Also called *plaintext*.

CLI
command-line interface. The primary interface for entering configuration and monitoring commands to the router. Refer to the Configuration Guide for the router you are configuring for information on what commands you can enter from the CLI.

client/server computing
Term used to describe distributed computing (processing) network systems in which transaction responsibilities are divided into two parts: client (front end) and server (back end). Also called distributed computing. See also RPC.

CM
WAAS central manager. Each WAE-E must register with the WAAS CM in order to be able to communicate with the WAE-C.

CME
Cisco Call Manager Express. CME provides call-processing services to voice over IP (VoIP) gateways.

CNS
Cisco Networking Services. A suite of services that support scalable network deployment, configuration, service-assurance monitoring, and service delivery.

comp-lzs
An IP compression algorithm.

Configuration, Config, Config File
The file on the router that holds the settings, preferences, and properties you can administer using Cisco SDM.

content engine
In the context of a WAAS solution, a cache of web content located on the network.

cookie
A cookie is a web browser feature which stores or retrieves information, such as a user's preferences, to persistent storage. In Netscape and Internet Explorer, cookies are implemented by saving a small text file on your local hard drive. The file can be loaded the next time you run a Java applet or visit a website. In this way information unique to you as a user can be saved between sessions. The maximum size of a cookie is approximately 4KB.

CPE
customer premises equipment.

CRL
certificate revocation list. A list maintained and signed by a certificate authority (CA) of all the unexpired but revoked digital certificates.

cryptography
Mathematical and scientific techniques for keeping data private, authentic, unmodified, and non-repudiated.

crypto map	In Cisco SDM, crypto maps specify which traffic should be protected by IPSec, where IPSec-protected traffic should be sent, and what IPSec transform sets should be applied to this traffic.
cTCP	Cisco Tunneling Control Protocol. cTCP is also called TCP over IPSec, or TCP traversal. cTCP is a protocol that encapsulates ESP and IKE traffic in the TCP header, so that firewalls in between the client and the server or headend device permit this traffic, considering it as TCP traffic.

D

data confidentiality	The result of data encryption that prevents the disclosure of information to unauthorized individuals, entities, or processes. This information can be either data at the application level, or communication parameters. See traffic flow confidentiality or traffic analysis.
data integrity	The presumed accuracy of transmitted data — signifying the sender's authenticity and the absence of data tampering.
data origin authentication	One function of a non-repudiation service.
decryption	Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.
default gateway	The gateway of last resort. The gateway to which a packet is routed when its destination address does not match any entries in the routing table.
delta file	A file that Cisco IOS IPS creates to store changes made to signatures.
DES	Data Encryption Standard. Standard cryptographic algorithm developed and standardized by the U.S. National Institute of Standards and Technology (NIST). Uses a secret 56-bit encryption key. The DES algorithm is included in many encryption standards.
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses to hosts dynamically, so that addresses can be reused when hosts no longer need them.

DH, Diffie-Hellman	A public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange.
Diffie-Hellman key exchange	A public key cryptography protocol that allows two parties to establish a shared secret over insecure communication channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange. Cisco IOS software supports 768-bit and 1024-bit Diffie-Hellman groups.
digest	The output of a hash function.
digital certificate	A cryptographically signed, digital representation of user or device attributes that binds a key to an identity. A unique certificate attached to a public key provides evidence that the key has not been compromised. A certificate is issued and signed by a trusted certification authority, and binds a public key to its owner. Certificates typically include the owner's name, the owner's public key, the certificate's serial number, and the certificate's expiration date. Other information might also be present. See X.509.
digital signature	An authentication method that permits the easy discovery of data forgery, and prevents repudiation. Additionally, the use of digital signatures allows for verification that a transmission has been received intact. Typically includes a transmission time stamp.
distributed key	A shared cryptographic key that is divided into pieces, with each piece provided to a different participant.
DLCI	data-link connection identifier. In Frame Relay connections, the identifier for a particular data link connection between two endpoints.
DMVPN	Dynamic multipoint virtual private network. A virtual private network in which routers are arranged in a logical hub and spoke topology, and in which the hubs have point-to-point GRE over IPSec connections with the hub. DMVPN uses GRE and NHRP to enable the flow of packets to destinations in the network.
single DMVPN	A router with a single DMVPN configuration has a connection to one DMVPN hub, and has one configured GRE tunnel for DMVPN communication.The GRE tunnel addresses for the hub and spokes must be in the same subnet.

DMZ   demilitarized zone. A DMZ is a buffer zone between the Internet, and your private networks. It can be a public network typically used for Web, FTP and E-Mail servers that are accessed by external clients on the Internet. Placing these public access servers on a separate isolated network provides an extra measure of security for your internal network.

DN   Distinguished Name. A unique identifier for a Certification Authority customer, included in each of that customer's certificates received from that Certification Authority. The DN typically includes the user's common name, the name of that user's company or organization, the user's two-letter country code, an e-mail address used to contact the user, the user's telephone number, the user's department number, and the city in which the user resides.

DNS   Domain Name System (or Service). An Internet service that translates domain names, which are composed of letters, into IP addresses, which are composed of numbers.

domain name   The familiar, easy-to-remember name of a host on the Internet that corresponds to its IP address.

DPD   dead peer detection. DPD determines if a peer is still active by sending periodic keepalive messages to which the peer is supposed to respond. If the peer does not respond within a specified amount of time, the connection is terminated.

DRAM   dynamic random access memory. RAM that stores information in capacitors that must be periodically refreshed.

DSCP   Differentiated Services Code Point. DSCP markings can be used to classify traffic for QoS. See also NBAR

DSLAM   digital subscriber line access multiplexer.

DSS   digital signature standard. Also called *digital signature algorithm* (DSA), the DSS algorithm is part of many public-key standards for cryptographic signatures.

DVTI	Dynamic Virtual Tunnel Interface. A DVTI is a routable interface that is able to selectively send traffic to different destinations. DVTIs are not statically mapped to physical interfaces. Thus they are able to send and receive encrypted data over any physical interface.
dynamic routing	Routing that adjusts automatically to network topology or traffic changes. Also called adaptive routing.

E

E1	A wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps.
EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol. Sometimes shortened to EOU. The protocol used by a client and a NAD to perform posture validation.
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling. A 802.1x EAP type developed by Cisco Systems to enable customers who cannot enforce strong password policies to deploy an 802.1x EAP type that does not require digital certificates.
Easy VPN	A centralized VPN management solution based on the Cisco Unified Client Framework.A Cisco Easy VPN consists of two components: a Cisco Easy VPN Remote client, and a Cisco Easy VPN server.
ECHO	See ping, ICMP.
eDonkey	Also known as eDonkey 2000 or ED2K is an extremely large peer-to-peer file sharing network. eDonkey implements the (Multisource File Transmission Protocol (MFTP).
EIGRP	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco Systems. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.

encapsulation	Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.
encrypt	To crytographically produce ciphertext from plaintext.
encryption	Application of a specific algorithm to data so as to alter the appearance of the data, making it incomprehensible to those who are not authorized to see the information.
enrollment proxy host	The proxy server for a certificate enrollment server.
enrollment URL	The enrollment URL is the HTTP path to a certification authority (CA) that your Cisco IOS router should follow when sending certificate requests. The URL includes either a DNS name or an IP address, and may be followed by a full path to the CA scripts.
ERR	Event Risk Rating. ERR is used to control the level at which a user chooses to take actions in an effort to minimize false positives.
ESP	Encapsulating Security Payload. An IPSec protocol that provides both data integrity and confidentiality. Also known as Encapsulating Security Payload, ESP provides confidentiality, data origin authentication, replay-detection, connectionless integrity, partial sequence integrity, and limited traffic flow confidentiality.
ESP_SEAL	ESP with the 160-bit key SEAL (Software Encryption Algorithm) encryption algorithm. This feature was introduced in 12.3(7)T. The router must not have hardware IPSec encryption enabled in order to use this feature.
esp-3des	ESP (Encapsulating Security Payload) transform with the 168-bit DES encryption algorithm (3DES or Triple DES).
esp-des	ESP (Encapsulating Security Payload) transform with the 56-bit DES encryption algorithm.
ESP-MD5-HMAC	ESP (Encapsulating Security Payload) transform using the MD5-variant SHA authentication algorithm.

esp-null	ESP (Encapsulating Security Payload) transform that provides no encryption and no confidentiality.
ESP-SHA-HMAC	ESP (Encapsulating Security Payload) transform using the HMAC-variant SHA authentication algorithm.
Ethernet	A widely used LAN protocol invented by Xerox Corporation, and developed by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD, and run over a variety of cable types at 10 Mbps, or at 100 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.
Event action override **event action override**	Event action overrides are used in IOS IPS 5.x. They allow you to change the actions associated with an event based on the RR of that event.
expiration date	The expiration date within a certificate or key indicates the end of its limited lifetime. The certificate or key is not trusted after its expiration date passes.
exception list	In a NAC implementation, a list of hosts with static addresses that are allowed to bypass the NAC process. These hosts may be placed on the exception list because they do not have posture agents installed, or because they are hosts such as printers or Cisco IP phones.
extended rules	A type of Access rule. Extended rules extended rules can examine a greater variety of packet fields to determine a match. Extended rules can examine both the packet's source and destination IP addresses, the protocol type, the source and destination ports, and other packet fields.
SDP	Secure Device Provisioning. SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server.

F

fasttrack	A file-sharing network in which indexing functions are dynamically assigned to connected peers, called supernodes.

fidelity rating	A number from 1 to 100 that indicates the confidence the rater has that a signature will generate an accurate alert.
finger	A software tool for determining whether a person has an account at a particular Internet site. Many sites do not allow incoming finger requests.
fingerprint	The fingerprint of a CA certificate is the string of alphanumeric characters that results from an MD5 hash of the whole CA certificate. Entities receiving a CA certificate can verify its authenticity by comparing it to its known fingerprint. This authentication is intended to ensure the integrity of communication sessions by preventing "man-in-the-middle" attacks.
firewall	A router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
Flash **Flash memory**	A memory chip which retains data without power. Software images can be stored in, booted from, and written to Flash as necessary.
Frame Relay	Industry standard, switched data link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement.
FTP	File Transfer Protocol. Part of the TCP/IP protocol stack, used for transferring files between hosts.

G

global IKE policy	An IKE policy that is global to a device, rather than affecting only a single interface on that device.
gnutella	A decentralized P2P file sharing protocol. Using an installed Gnutella client, users can search, download and upload files across the Internet.

GRE	generic routing encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.
GRE over IPSec	This technology uses IPSec to encrypt GRE packets.
G.SHDSL	Also known as G.991.2, G.SHDSL is an international standard for symmetric DSL developed by the International Telecommunications Union. G.SHDSL provides for sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 kbps and 2.31 Mbps.

H

H.323	An ITU-T standard that enables video conferencing over local-area networks (LANs) and other packet-switched networks, as well as video over the Internet.
hash	One-way process that converts input of any size into checksum output of a fixed size, called a *message digest*, or just a *digest*. This process is not reversible, and it is not feasible to create or modify data to result in a specific digest.
hash algorithm	A hash algorithm is used to generate a hash value, also known as a message digest, ensures that message contents are not changed during transmission. The two most widely used types of hash algorithms are Secure Hash Algorithm (SHA) and MD5
HDLC	High-Level Data Link Control. Bit-oriented synchronous data link layer protocol developed by the International Standards Organization (ISO). HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.
headend	The upstream, transmit end of a tunnel.

HMAC	Hash-based Message Authentication Code. HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.
HMAC-MD5	Hashed Message Authentication Codes with MD5 (RFC 2104). A keyed version of MD5 that enables two parties to validate transmitted information using a shared secret.
host	A computer, such as a PC, or other computing device, such as a server, associated with an individual IP address and optionally a name. The name for any device on a TCP/IP network that has an IP address. Also any network-addressable device on any network. The term *node* includes devices such as routers and printers which would not normally be called *hosts*.
HTTP **HTTPS**	Hypertext Transfer Protocol, Hypertext Transfer Protocol, Secure. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
hub	In a DMVPN network, a hub is a router with a point-to-point IPSec connection to all spoke routers in the network. The hub is the logical center of a DMVPN network.

I

ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
Identical Addressing	The ability to reach devices having identical IP addresses over an EasyVPN connection through the use of Network Address Translation.
IDS	Intrusion Detection System. The Cisco IPS performs a real time analysis of network traffic to find anomalies and misuse, using a library of signatures it can compare traffic against. When it finds unauthorized activity or anomalies, it can terminate the condition, block traffic from attacking hosts, and send alerts to the IDM.

IDS Sensor   An IDS sensor is hardware on with the Cisco IDS runs. IDS sensors can be stand-alone devices, or network modules installed on routers.

IDM   IDS Device Manager. IDM is software used to manage an IDS sensor.

IEEE   Institute of Electrical and Electronics Engineers.

IETF   Internet Engineering Task Force.

IGMP   Internet Group Management Protocol. IGMP is a protocol used by IPv4 systems to report IP multicast memberships to neighboring multicast routers

IKE   Internet Key Exchange. IKE is a key management protocol standard used in conjunction with IPSec and other standards. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

IKE negotiation   A method for the secure exchange of private keys across non-secured networks.

IKE profile   A group of ISAKMP parameters that can be mapped to different IP Security tunnels.

IM   Instant Messaging. A real-time communication service in which both parties are online at the same time. Popular IM services include Yahoo! Messenger (YM), Microsoft Networks Messenger, and AOL Instant Messenger (AIM).

IMAP   Internet Message Access Protocol. A protocol used by clients to communicate with an e-mail server. Defined in RFC 2060, IMAP enables clients to delete, change the status, and otherwise manipulate messages on the e-mail server as well as retrieve them.

implicit rule   An access rule automatically created by the router based on default rules or as a result of user-defined rules.

inside global   The IP address of a host inside a network as it appears to devices outside the network.

inside local   The configured IP address assigned to a host inside the network.

inspection rule   A CBAC inspection rule allows the router to inspect specified outgoing traffic so that it can allow return traffic of the same type that is associated with a session started on the LAN. If a firewall is in place, incoming traffic that is associated with a session started inside the firewall might be dropped if an inspection rule has not been configured.

interface   The physical connection between a particular network and the router. The router's LAN interface connects to the local network that the router serves. The router has one or more WAN interfaces that connect to the Internet.

Internet   The global network which uses IP, Internet protocols. Not a LAN. See also intranet.

intranet   Intranetwork. A LAN which uses IP, and Internet protocols, such as SNMP, FTP, and UDP. See also network, Internet.

IOS   Cisco IOS software. Cisco system software that provides common functionality, scalability, and security for all products under CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services and platforms.

IOS IPS   Cisco IOS Intrusion Prevention System. IOS IPS compares traffic against an extensive database of intrusion signatures, and can drop intruding packets and
IPS   take other actions based on configuration. Signatures are built in to IOS images supporting this feature, and additional signatures can be stored in local or remote signature files.

IP   Internet Protocol. The Internet protocols are the world's most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications.

IP address	IP version 4 addresses are 32 bits, or 4 bytes, in length. This address "space" is used to designate the network number, the optional subnetwork number, and a host number. The 32 bits are grouped into four octets (8 binary bits), represented by 4 decimal numbers separated by periods or "dots." The part of the address used to specify the network number, the subnetwork number, and the host number is specified by the subnet mask.
IPSec	A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
IPSec policy	In Cisco SDM, an IPSec policy is a named set of crypto map associated with a VPN connection.
IPSec rule	A rule used to specify which traffic is protected by IPSec.
IRB	Integrated Routing and Bridging. IRB allows you to route a given protocol between routed interfaces and bridge groups within a single switch router.
ISAKMP	The Internet Security Association Key Management Protocol is the basis for IKE. ISAKMP authenticates communicating peers, creates and manages security associations, and defines key generation techniques.

K

kazaa2	A peer-to-peer file sharing service.
key	A string of bits used to encrypt or decrypt data, or to compute message digests.
key agreement	The process whereby two or more parties agree to use the same secret symmetric key.
key escrow	A trusted third party who holds the cryptographic keys.

key exchange	The method by which two or more parties exchange encryption keys. The IKE protocol provides one such method.
key lifetime	An attribute of a key pair that specifies a time span, during which the certificate containing the public component of that key pair is considered valid.
key management	The creation, distribution, authentication, and storage of encryption keys.
key pair	See public key encryption.
key recovery	A trusted method by which encrypted information can be decrypted if the decryption key is lost or destroyed.

L

L2F Protocol	Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.
L2TP	Layer 2 Tunneling Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN. L2TP is proposed as an IPSec alternative, but is used sometimes alongside IPSec to provide authentication services.
LAC	L2TP access concentrator. Device terminating calls to remote systems and tunneling PPP sessions between remote systems and the LNS.
LAN	Local Area Network. A network residing in one location or belonging to one organization, typically, but not necessarily using IP and other Internet protocols. Not the global Internet. *See also* intranet, network, Internet.
LAPB	Link Access Procedure, Balanced.
Layer 3 Interface	Layer 3 interfaces support internetwork routing. A VLAN is an example of a logical layer 3 interface. An Ethernet port is an example of a physical layer 3 interface.
LBO	Line Build Out.

LEFS	low-end file system.
life cycle	See expiration date.
LLQ	Low Latency Queuing (LLQ) allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.
LNS	L2TP network server. Device able to terminate L2TP tunnels from a LAC and able to terminate PPP sessions to remote systems through L2TP data sessions.
local subnet	Subnetworks are IP networks arbitrarily segmented by a network administrator (by means of a subnet mask) in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. The local subnet is the subnet associated with your end of a transmission.
logical interface	An interface that has been created solely by configuration, and that is not a physical interface on the router. Dialer interfaces and tunnel interfaces are examples of logical interfaces.
loopback	In a loopback test, signals are sent and then redirected back toward their source from some point along the communications path. Loopback tests are often used to determine network interface usability.

M

MAC	message authentication code. The cryptographic checksum of the message used to verify message authenticity. See hash.

mask

subnet mask

netmask

network mask

A 32-bit bit mask which specifies how an Internet address is to be divided into network, subnet, and host parts. The net mask has ones (1's) in the bit positions in the 32-bit address that are to be used for the network and subnet parts, and has zeros (0's) for the host part. The mask should contain at least the standard network portion (as determined by the address class), and the subnet field should be contiguous with the network portion. The mask is configured using the decimal equivalent of the binary value.

Examples:

Decimal: 255.255.255.0
Binary: 11111111 11111111 11111111 00000000
The first 24 bits provide the network and subnetwork address, and the last 8 provide the host address.

Decimal: 255.255.255.248
Binary: 11111111 11111111 11111111 11111000
The first 29 bits provide the network and subnetwork address, and the last 3 provide the host address.

See also IP Address, TCP/IP, host, host/network.

MD5

Message Digest 5. A one-way hashing function that produces a 128-bit hash. Both MD5 and Secure Hashing Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. MD5 verifies the integrity and authenticates the origin of a communication.

message digest

A string of bits that represents a larger data block. This string defines a data block, based on the processing of its precise content through a 128-bit hash function. Message digests are used in the generation of digital signatures. See hash.

MD5

Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

mGRE	multipoint GRE.
MTU	maximum transmission unit. The maximum packet size, in bytes that an interface can transmit or receive.

N

NAC	Network Admission Control. A method of controlling access to a network in order to prevent the introduction of computer viruses. Using a variety of protocols and software products, NAC assesses the condition of hosts when they attempt to log onto the network, and handles the request based on the host's condition, called its *posture*. Infected hosts can be placed in quarantine; hosts without up-to-date virus protection software can be directed to obtain updates, and uninfected hosts with up-to-date virus protection can be allowed onto the network. See also ACL, posture, and EAPoUDP.
NAD	Network Access Device. In a NAC implementation, the device that receives a host's request to log on to the network. A NAD, usually a router, works with posture agent software running on the host, virus protection software, and ACS and posture/remediation servers on the network to control access to the network in order to prevent infection by computer viruses.
NAS	Network Access Server. Platform that interfaces between the Internet and the public switched telephone network (PSTN).
	Gateway that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs both synchronous and asynchronous routing of supported protocols.
NAT **Network Address Translation**	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
NBAR	Network-based Application Recognition. A method used to classify traffic for QoS.

NetFlow A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.

network A network is a group of computing devices which share part of an IP address space and not a single host. A network consists of multiple "nodes" or devices with IP address, any of which may be referred to as *hosts*. See also Internet, Intranet, IP, LAN.

network bits In a subnet mask, the number of bits set to binary 1. A subnet mask of 255.255.255.0 has 24 network bits, because 24 bits in the mask are set to 1. A subnet mask of 255.255.248 has 17 network bits.

network module A network interface card that is installed in the router chassis to add functionality to the router. Examples are Ethernet network modules, and IDS network modules.

NHRP Next Hop Resolution protocol. A client and server protocol used in DMVPN networks, in which the hub router is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes in order to build direct tunnels to them.

non-repudiation service A third-party security service that stores evidence for later, possible retrieval, regarding the origin and destination of all data included in a communication — without storing the actual data. This evidence can be used to safeguard all participants in that communication against false denials by any participant of having sent information, as well as false denials by any participant of having received information.

NTP Network Time Protocol. A protocol to synchronize the system clocks on network devices. NTP is a UDP protocol.

NVRAM Non-volatile random access memory.

O

Oakley   A protocol for establishing secret keys for use by authenticated parties, based on Diffie-Hellman and designed to be a compatible component of ISAKMP.

OFB   output feedback. An IPSec function that feeds encrypted output (generally, but not necessarily, DES-encrypted) back into the original input. Plaintext is encrypted directly with the symmetric key. This produces a pseudo-random number stream.

outside global   The IP address assigned to a host on the outside network by the host's owner. The address was allocated from globally routable address or network space.

outside local   The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from an address space routable on the inside.

OSPF   Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

P

P2P   See peer-to-peer.

PAD   packet assembler/disassembler. Device used to connect simple devices (like character-mode terminals) that do not support the full functionality of a particular protocol to a network. PADs buffer data and assemble and disassemble packets sent to such end devices.

padding   In cryptosystems, *padding* refers to random characters, blanks, zeros, and nulls added to the beginning and ending of messages, to conceal their actual length or to satisfy the data block size requirements of some ciphers. Padding also obscures the location at which cryptographic coding actually starts.

PAM   Port to Application Mapping. PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

PAP	Password Authentication Protocol. An authentication protocol that allows peers to authenticate one another. PAP passes the password and hostname or username in unencrypted form. See also CHAP.
parameter map	Parameter-maps specify inspection behavior for Zone-Policy Firewall, for parameters such as Denial-of-Service Protection, session and connection timers, and logging settings. Parameter-maps are also applied with Layer 7 class- and policy-maps to define application-specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application-specific information.
password	A protected and secret character string (or other data source) associated with the identity of a specific user or entity.
password aging **Password aging**	The ability of a system to notify a user that their password has expired, and to provide them with themeans to create a new password.
PAT **Dynamic PAT**	Port Address Translation. Dynamic PAT lets multiple outbound sessions appear to originate from a single IP address. With PAT enabled, the router chooses a unique port number from the PAT IP address for each outbound translation slot (xlate). This feature is valuable when an Internet service provider cannot allocate enough unique IP addresses for your outbound connections. The global pool addresses always come first, before a PAT address is used.
peer	In IKE, peers are routers acting as proxies for the participants in an IKE tunnel. In IPSec, peers are devices or entities that communicate securely either through the exchange of keys or the exchange of digital certificates.
peer-to-peer	A type of network design where all hosts share roughly equivalent capabilities. Also called P2P, peer-to-peer networking is used by many file sharing networks.
PEM	Privacy Enhanced Mail format. A format for storing digital certificates.
PFS	perfect forward secrecy. A property of some asymmetric key agreement protocols that allows for the use of different keys at different times during a session, to ensure that the compromising of any single key will not compromise the session as a whole.
physical interface	A router interface supported by a network module that is installed in the router chassis, or that is part of the router's basic hardware.

ping An ICMP request sent between hosts to determine whether a host is accessible on the network.

PKCS7 Public Key Cryptography Standard Number 7.

PKCS12 Public Key Cryptography Standard Number 12. A format for storing digital certificate information. See also PEM.

PKI public-key infrastructure. A system of certification authorities (CAs) and registration authorities (RAs) that provides support for the use of asymmetric key cryptography in data communication through such functions as certificate management, archive management, key management, and token management.

Alternatively, any standard for the exchange of asymmetric keys.

This type of exchange allows the recipient of a message to trust the signature in that message, and allows the sender of a message to encrypt it appropriately for the intended recipient. See key management.

plaintext Ordinary, unencrypted data.

police rate The rate of bits per second that traffic must not exceed.

policing Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped, or remarked.

policy map A policy map consists of configured actions to be taken on traffic. Traffic is defined in a class map. More than one class map can be associated with a policy map.

POP3 Post Office Protocol version 3. A protocol used to retrieve e-mail from an e-mail server.

posture In a NAC implementation, the condition of a host attempting access to the network. Posture agent software running on the host communicates with the NAD to report on the host's compliance with the network security policy.

PPP Point-to-Point Protocol. A protocol that provides router-to-router, and host-to-network connections over synchronous and asynchronous circuits. PPP has built in security mechanisms, such as CHAP and PAP.

PPPoA   Point-to-Point Protocol over Asynchronous Transfer Mode (ATM). Primarily implemented as part of ADSL, PPPoA relies on RFC1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode.

PPPoE   Point-to-Point Protocol over Ethernet. PPP encapsulated in Ethernet frames. PPPoE enables hosts on an Ethernet network to connect to remote hosts through a broadband modem.

PPTP   Point-to-Point Tunneling Protocol. Creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over TCP/IP-based networks. Can be used as an alternative to the L2F and L2TP tunneling protocols. Proprietary Microsoft protocol.

pre-shared key One of three authentication methods offered in IPSec, with the other two methods being RSA encrypted nonces, and RSA signatures. Pre-shared keys allow for one or more clients to use individual shared secrets to authenticate encrypted tunnels to a gateway using IKE. Pre-shared keys are commonly used in small networks of up to 10 clients. With pre-shared keys, there is no need to involve a CA for security.

The Diffie-Hellman key exchange combines public and private keys to create a shared secret to be used for authentication between IPSec peers. The shared secret can be shared between two or more peers. At each participating peer, you would specify a shared secret as part of an IKE policy. Distribution of this pre-shared key usually takes place through a secure out-of-band channel. When using a pre-shared key, if one of the participating peers is not configured with the same pre-shared key, the IKE SA cannot be established. An IKE SA is a prerequisite to an IPSec SA. You must configure the pre-shared key at all peers.

Digital certification and wildcard pre-shared keys (which allow for one or more clients to use a shared secret to authenticate encrypted tunnels to a gateway) are alternatives to pre-shared keys. Both digital certification and wildcard pre-shared keys are more scalable than pre-shared keys.

private key   See public key encryption.

pseudo random   An ordered sequence of bits that appears superficially similar to a truly random sequence of the same bits. A key generated from a pseudo random number is called a nonce.

public key encryption	In public key encryption systems, every user has both a public key and a private key. Each private key is maintained by a single user and shared with no one. The private key is used to generate a unique digital signature and to decrypt information encrypted with the public key. In contrast, a user's public key is available to everyone to encrypt information intended for that user, or to verify that user's digital signature. Sometimes called public key cryptography.
PVC	permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

Q

QoS	Quality of Service. A method of guaranteeing bandwidth to specified types of traffic.
queuing	Traffic queuing aggregates packet streams to multiple queues and provides different service to each queue. See also LLQ and CBWFQ.
quick mode	In Oakley, the name of the mechanism used after a security association has been established to negotiate changes in security services, such as new keys.

R

RA	registration authority. An entity serving as an optional component in PKI systems to record or verify some of the information that certification authorities (CAs) use when issuing certificates or performing other certificate management functions. The CA itself might perform all RA functions, but they are generally kept separate. RA duties vary considerably, but may include assigning distinguished names, distributing tokens, and performing personal authentication functions.
RADIUS	Remote Authentication Dial-In User Service. An access server authentication and accounting protocol that uses UDP as the transport protocol. See also TACACS+

RCP　　　　　　　remote copy protocol. Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data

remote subnet　　Subnetworks are IP networks arbitrarily segmented by a network administrator (by means of a subnet mask) in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. A "remote subnet" is the subnet that is *not* associated with your end of a transmission.

replay-detection　A standard IPSec security feature that combines sequence numbers with authentication, so the receiver of a communication can reject old or duplicate packets in order to prevent replay attacks.

repudiation　　　In cryptographic systems, repudiation is the denial by one of the entities involved in a communication of having participated in all or part of that communication.

revocation password　The password that you provide to a CA when you request that it revoke a router's digital certificate. Sometimes called a *challenge password*.

RFC 1483 routing　RFC1483 describes two different methods for carrying connectionless network interconnect traffic over an ATM network: routed protocol data units (PDUs) and bridged PDUs. Cisco SDM supports the configuration of RFC 1483 routing, and enables you to configure two encapsulation types: AAL5MUX, and AAL5SNAP.

AAL5MUX: AAL5 MUX encapsulation supports only a single protocol (IP or IPX) per PVC.

AAL5SNAP: AAL5 Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) encapsulation supports Inverse ARP and incorporates the LLC/SNAP that precedes the protocol datagram. This allows the multiple protocols to transverse the same PVC.

RIP　　　　　　　Routing Information Protocol. A routing protocol that uses the number of routers a packet must pass through to reach the destination, as the routing metric.

root CA　　　　　Ultimate certification authority (CA), which signs the certificates of the subordinate CAs. The root CA has a self-signed certificate that contains its own public key.

route	A path through an internetwork.
route map	Route maps enable you to control information that is added to the routing table. Cisco SDM automatically creates route maps to prevent NAT from translating specific source addresses when doing so would prevent packets from matching criteria in an IPSec rule.
RPC	remote procedure call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the clients. See also client/server computing.
RR	Risk Rating. An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
RSA	Rivest, Shamir, and Adelman, the inventors of this cryptographic key exchange technique, which is based on factoring large numbers. RSA is also the name of the technique itself. RSA may be used for encryption and authentication, and is included in many security protocols.
RSA keys	An RSA asymmetric key pair is a set of matching public and private keys.
RSA signatures	One of three authentication methods offered in IPSec, with the other two methods being RSA encrypted nonces, and pre-shared keys. Also, one of the three Federal Information Processing Standards (FIPS)–approved algorithms for generating and verifying digital signatures. The other approved algorithms are DSA and Elliptic Curve DSA.
rule	Information added to the configuration to define your security policy in the form of conditional statements that instruct the router how to react to a particular situation.

S

SA security association. A set of security parameters agreed upon by two peers to protect a specific session in a particular tunnel. Both IKE and IPSec use SAs, although SAs are independent of one another.

IPSec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

A set of SAs is needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Protocol (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

SAID security association ID. Numeric identifier for the SA of a given link.

salt A string of pseudorandom characters used to enhance cryptographic complexity.

SCCP Skinny Client Control Protocol. SCCP is a proprietary terminal control protocol owned by Cisco Systems. It is used as a messaging protocol between a skinny client and Cisco CallManager.

SDEE Security Device Event Exchange. A message protocol that can be used to report on security events, such as alarms generated when a packet matches the characteristics of a signature.

SDF Signature Definition File. A file, usually in XML format, containing signature definitions that can be used to load signatures on a security device.

SEAF Signature Event Action Filter. A filter that allows you to subtract actions from an event whose parameters fall within those defined. For example, a SEAF can be created to subtract the action Reset TCP Connection from an event associated with a particular attacker address.

SEAO	Signature Event Action Override. An SEAO allows you to assign a risk rating (RR) range to an IPS event action type, such as alarm. If an event occurs with an RR in the range you have assigned to the action type, then that action is added to the event. In this case, an alarm would be added to the event.
SEAP	Signature Event Action Processor. SEAP allows filtering and overrides based on Event Risk Rating (ERR) feedback.
secret key	See symmetric key.
security association lifetime	The predetermined length of time in which an SA is in effect.
security zone	A group of interfaces to which a policy can be applied. Security zones should consist of interfaces that share similar functions or features. For example, on a router, interfaces Ethernet 0/0 and Ethernet 0/1 may be connected to the local LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.
session key	A key that is used only once.
SFR	Signature Fidelity Rating. A weight associated with how well this signature might perform in the absence of specific knowledge of the target.
SHA	Some encryption systems use the Secure Hashing Algorithm to generate digital signatures, as an alternative to MD5.
SHA-1	Secure Hashing Algorithm 1. Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.
shaping	Traffic shaping retains excess packets in a queue and then reschedules the excess for later transmission over increments of time.
shared key	The secret key that all users share in a symmetric key-based communication session.
shared secret	A crytographic key.

signature	A data element in IOS IPS that detects a specific pattern of misuse on the network.
signature engine	A signature engine is a component of Cisco IOS IPS designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters which have allowable ranges or sets of values.
signing certificate	Used to associate your digital signature with your messages or documents, and to ensure that your messages or files are conveyed without changes.
SIP	Session Initiation Protocol. Enables call handling sessions, particularly two-party audio conferences, or "calls." SIP works with Session Description Protocol (SDP) for call signaling. SDP specifies the ports for the media stream. Using SIP, the router can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers.
site-to-site VPN	Typically, a site-to-site VPN is one that connects two networks or subneworks and that meets several other specific criteria, including the use of static IP addresses on both sides of the tunnel, the absence of VPN client software on user end-stations, and the absence of a central VPN hub (as would exist in hub-and-spoke VPN configurations). Site-to-site VPNs are not intended to replace dial-in access by remote or traveling users.
SMTP	Simple Mail Transfer Protocol. Internet protocol providing e-mail services.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SPD	Selective Packed Discard. SPD provides priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of queue congestion.
Split DNS	Split DNS enables Cisco routers to answer DNS queries using the internal hostname cache specified by a selected virtual DNS name server. Queries that cannot be answered by the information in the hostname cache, are redirected to specified back-end DNS name servers.

spoke	In a DMVPN network, a spoke router is a logical end point in the network, and has a point-to-point IPSec connection with a DMVPN hub router.
spoofing **spoof**	The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms such as filters and access lists.
SRB	source-route bridging. Method of bridging originated by IBM and popular in Token Ring networks. In an SRB network, the entire route to a destination is predetermined, in real time, prior to the sending of data to the destination.
SSH	Secure Shell. An application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. Up to five SSH clients are allowed simultaneous access to the router console.
SSID	Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
SSL VPN	Secure Socket Layer Virtual Private Networks. SSL VPN is a feature that enables a supported Cisco router to provide remote clients secure access to network resources by creating an encryption tunnel across the Internet using the broadband or ISP dial connection that the remote client uses.
SSL VPN context	A WebVPN context provides the resources needed to configure secure access to a corporate intranet and other types of private networks. A WebVPN context must include an associated WebVPN gateway. A WebVPN context can serve one or more WebVPN group policies.
SSL VPN gateway	A WebVPN gateway provides an IP address and a certificate for a WebVPN context. The
SSL VPN group policy	WebVPN group policies define the portal page and links for the users included in those policies. A WebVPN group policy is configured under a WebVPN context.

standard rule	In Cisco SDM, a type of access rule or NAT rule. Standard rules compare a packet's source IP address against its IP address criteria to determine a match.Standard rules use a wildcard mask to determine which portions of the IP address must match.
state, stateful, stateful Inspection	Network protocols maintain certain data, called state information, at each end of a network connection between two hosts. State information is necessary to implement the features of a protocol, such as guaranteed packet delivery, data sequencing, flow control, and transaction or session IDs. Some of the protocol state information is sent in each packet while each protocol is being used. For example, a web browser connected to a web server uses HTTP and supporting TCP/IP protocols. Each protocol layer maintains state information in the packets it sends and receives. Routers inspect the state information in each packet to verify that it is current and valid for every protocol it contains. This is called stateful inspection and is designed to create a powerful barrier to certain types of computer security threats
Static PAT	Static Port Address Translation. A static address maps a local IP address to a global IP address. Static PAT is a static address that also maps a local port to a global port. See also PAT.
static route	Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.
subnet, subnetwork	In IP networks, a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by the network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. See also IP address, subnet bits, subnet mask.
subnet bits **subnet mask**	32-bit address mask used in IP to indicate the bits of an IP address that are being used for the network and optional subnet address. Subnet masks are expressed in decimal. The mask 255.255.255.0 specifies that the first 24 bits of the address Sometimes referred to simply as mask. See also address mask and IP address.
SUNRPC	SUN Remote Procedure Call. RPC is a protocol that allows clients to run programs or routines on remote servers. SUNRPC is the version of RPC originally distributed in the SUN Open Network Computing (ONC) library.
symmetric key	A symmetric key is used to decrypt information that it previously encrypted.

T

T1	A T1 link is a data link capable of transmitting data at a rate of 1.5 MB per second.
TACACS+	Terminal Access Controller Access Control System plus. An access server authentication and accounting protocol that uses TCP as the transport protocol.
tail-end	The downstream, receive end of a tunnel.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
TCP Syn Flood Attack	A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a website, accessing e-mail, using FTP service, and so on.
Telnet	A terminal emulation protocol for TCP/IP networks such as the Internet. Telnet is a common way to control web servers remotely.
TFTP	Trivial File Transfer Protocol. TFTP is a simple protocol used to transfer files. It runs on UDP and is explained in depth in Request For Comments (RFC) 1350.
traffic flow confidentiality or traffic analysis	Security concept that prevents the unauthorized disclosure of communication parameters. The successful implementation of this concept hides source and destination IP addresses, message length, and frequency of communication from unauthorized parties
transform	Description of a security protocol and its corresponding algorithms.
transform set	A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.
tunnel	A virtual channel through a shared medium such as the Internet, used for the exchange of encapsulated data packets.

tunneling   The process of piping the stream of one protocol through another protocol.

TVR   Target Value Rating. The TVR is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

U

UDP   User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol that belongs to the Internet protocol family.

unencrypted   Not encrypted.

Unity Client   A client of a Unity Easy VPN Server.

URI   Uniform Resource Identifier. Type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. [RFC 1630]

URL   Universal Resource Locator. A standardized addressing scheme for accessing hypertext documents and other services using a browser. Two examples follow:

                       http://www.cisco.com.

                       ftp://10.10.5.1/netupdates/sig.xml

V

verification   Identity confirmation of a person or process.

VCI   virtual channel identifier. A virtual path may carry multiple virtual channels corresponding to individual connections. The VCI identifies the channel being used. The combination of VPI and VCI identifies an ATM connection.

VFR	Virtual Fragment Reassembly. VFR enables IOS Firewall to dynamically create ACLs to block IP fragments. IP fragments often do not contain enough information for static ACLs to be able to filter them.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network.
VPI	virtual path identifier. Identifies the virtual path used by an ATM connection.
VPDN	virtual private dial-up network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the home gateway, instead of the network access server (NAS).
VPN	Virtual Private Network. Provides the same network connectivity for users over a public infrastructure as they would have over a private network. VPNs enable IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
VPN connection	A site-to-site VPN. A site-to-site VPN consists of a set of VPN connections between peers, in which the defining attributes of each connection include the following device configuration information:

- A connection name
- Optionally, an IKE policy and pre-shared key
- An IPSec peer
- A list of one or more remote subnets or hosts that will be protected by the connection
- An IPSec rule that defines which traffic is to be encrypted.
- A list of transform sets that define how protected traffic is encrypted
- A list of the device network interfaces to which the connection is applied

VPN mirror policy	A VPN policy on a remote system that contains values that are compatible with a local policy and that enable the remote system to establish a VPN connection to the local system. Some values in a mirror policy must match values in a local policy, and some values, such as the IP address of the peer, must be the reverse of the corresponding values in the local policy.
	You can create mirror policies for remote administrators to use when you configure site-to-site VPN connections. For information on generating a mirror policy, refer to Generate Mirror....
VTI	Virtual Template Interface.
vty	virtual type terminal. Commonly used as virtual terminal lines.

W

WAN	Wide Area Network. A network that serves users across a broad geographical area, and often uses transmission devices provided by common carriers. See also LAN.
WAAS	Wide Area Application Services. A Cisco solution that optimizes the performance of TCP-based applications across a wide area network.
WCCP	Web Cache Communication Protocol. Also known as Web Cache Control Protocol and Web Cache Coordination Protocol. WCCP allows the use of a Content Engine to reduce Web traffic to reduce transmission costs and download time from Web servers.
WAE	Wide Area Application Engine. The term refers to Cis co network appliances that enable WAN optimization and application acceleration.
WAE-C	WAE-Core. The core WAE component is installed on a server at the data center. It connects directly to one or more file servers or network-attached storage (NAS) devices.
WAE-E	WAE-Edge. The edge WAE is installed on clients. It is a file caching device that serves client requests at remote sites and branch offices.

WFQ	Weighted Fair Queuing. A flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows.
wildcard mask	A bit mask used in access rules, IPSec rules, and NAT rules to specify which portions of the packet's IP address must match the IP address in the rule. A wildcard mask contains 32 bits, the same number of bits in an IP address. A wildcard bit value of 0 specifies that the bit in that same position of the packet's IP address must match the bit in the IP address in the rule. A value of 1 specifies that the corresponding bit in the packet's IP address can be either 1 or 0, that is, that the rule "doesn't care" what the value of the bit is. A wildcard mask of 0.0.0.0 specifies that all 32 bits in the packet's IP address must match the IP address in the rule. A wildcard mask of 0.0.255.0 specifies that the first 16 bits, and the last 8 bits must match, but that the third octet can be any value. If the IP address in a rule is 10.28.15.0, and the mask is 0.0.255.0, the IP address 10.28.88.0 would match the IP address in the rule, and the IP address 10.28.15.55 would not match.
WINS	Windows Internet Naming Service. A Windows system that determines the IP address associated with a particular network computer.
WMM	Wi-Fi Multimedia. An IEEE 802.11e Quality of Service (QoS) draft standard. WMM compliant equipment is designed to improve the user experience for audio, video, and voice applications over a Wi-Fi wireless connection.
WRED	Weighted Random Early Detection. A queueing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

X

X.509	A digital certificate standard, specifying certificate structure. Main fields are ID, subject field, validity dates, public key, and CA signature.
X.509 certificate	A digital certificate that is structured according to the X.509 guidelines.

X.509 certificate revocation list (CRL)   A list of certificate numbers that have been revoked. An X.509 CRL is one that meets either of the two CRL formatting definitions in X.509.

XAuth   IKE Extended Authentication. Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list-name must match the Xauth configuration list-name for user authentication to occur.

Xauth is an extension to IKE, and does not replace IKE authentication.

Z

zone   In a Zone-Based Policy Firewall, a zone is a group of interfaces that have similar functions or features. For example, if the interfaces FastEthernet 0/0 and FastEthernet 0/1 are both connected to the LAN, they could be grouped together in a single zone for the LAN.

zone-pair   A zone-pair allows you to specify a unidirectional traffic flow between two security zones. See also security zone

ZPF   Zone-Based Policy Firewall. In a ZPF configuration interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones.

I N D E X

Symbols

$ETH-LAN$ **1**

$ETH-WAN$ **3**

Numerics

3DES **9**

A

About SDM

    SDM version **2**

access rule

    in NAT translation rule **24, 27**

    making changes in firewall policy **6**

Access Rules window **3**

address pools **8, 15**

ADSL

    operating mode **19, 26**

ADSL operating mode

    adls2 **27**

    adsl2+ **27**

    ansi-dmt **26**

    itu-dmt **26**

    splitterless **27**

ADSL over ISDN

    default operating mode **19**

    operating modes **29**

AES encryption **9**

AH authentication **12**

ansi-dmt **26**

Application Traffic

    viewing activity **23**

ATM

    subinterface **2**

authentication

    AH **12**

    digital signatures **21**

    ESP **11**

    MD5 **9**

    SHA_1 **9**

AutoSecure **25**

B

banner, configuring **14, 30**

BOOTP, disabling **8**

X